COMMON DIRECTORY SERVICES AND PROCEDURES

ACP 133 Edition B

March 2000

(Reverse Blank)

replace this page with a blank one

FOREWORD

1. ACP 133, COMMON DIRECTORY SERVICES AND PROCEDURES, is an UNCLASSIFIED Allied Communication Publication (ACP). Periodic accounting of this publication is not required.

2. ACP 133 will be effective for National, Service, or Allied use when directed by the appropriate Implementing Agency; refer to the National Letter of Promulgation (LOP).

3. This publication contains Allied military information and is furnished for official purposes only.

4. This publication is not releasable without prior approval from the United States Military Communications-Electronic Board (USMCEB).

5. It is permitted to copy or make extracts from this publication without consent of the Authorizing Agency.

replace this page with a blank one

[US National LOP for ACP 133]

replace this page with a blank one

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
205 b		September 1999	ACP 133 Task Force
219, Table 2-3		September 1999	ACP 133 Task Force
227		September 1999	ACP 133 Task Force
303 j		September 1999	ACP 133 Task Force
305		September 1999	ACP 133 Task Force
307 a, b		September 1999	ACP 133 Task Force
308 c		September 1999	ACP 133 Task Force
308 e		September 1999	ACP 133 Task Force
310 a, b, c, e, f, i, j, k,		September 1999	ACP 133 Task Force
l, p, g, r		September 1999	ACP 133 Task Force
311 m, p		September 1999	ACP 133 Task Force
Tables 3-1, 3-2, 3-3, 3-4, 3-5, 3-7, 3-9, 3-10, 3-11, 3-12, 3-13, 3-15, 3-16, 3-18, 3-19		September 1999	ACP 133 Task Force
Annex A, 1 r, s, t, u, v, w, y, bb, dd, hh		September 1999	ACP 133 Task Force
Annex A, 1, renumbered ee - iii		September 1999	ACP 133 Task Force
Annex A, 2 b, d		September 1999	ACP 133 Task Force
Annex A, 2, renumbered c		September 1999	ACP 133 Task Force
Annex A, 4		September 1999	ACP 133 Task Force
Annex A, 5		September 1999	ACP 133 Task Force
Annex B, 1		September 1999	ACP 133 Task Force
Annex B, 1 c		September 1999	ACP 133 Task Force
Annex B, 3 b, e, i, j, n, o, p, q		September 1999	ACP 133 Task Force
Annex B, 4 b, c		September 1999	ACP 133 Task Force
Annex B, 5 a, b, c, i, j, k, p, q		September 1999	ACP 133 Task Force
Annex B, 5, renumbered l - w		September 1999	ACP 133 Task Force
Annex B, 5 l, m, n, o, p (1), r, s, t, u, v, w		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Annex B, 6 a		September 1999	ACP 133 Task Force
Annex B, 7		September 1999	ACP 133 Task Force
Annex B, 7 a, b, c, d, e, l, m		September 1999	ACP 133 Task Force
Annex B, 7, renumbered f - l, n - o		September 1999	ACP 133 Task Force
Annex B, 7 d (1), f, g, h, i, j, k, l (1), n		September 1999	ACP 133 Task Force
Annex B, 8 c		September 1999	ACP 133 Task Force
Annex B, 9		September 1999	ACP 133 Task Force
Annex B, 11 a, e		September 1999	ACP 133 Task Force
Annex B, 12 a, d, g, j, l, p, s, t, v, z, cc, ee, hh, ii, ll, nn,		September 1999	ACP 133 Task Force
Annex B, 12 cc (2)		September 1999	ACP 133 Task Force
Annex B, 12 ee (2)		September 1999	ACP 133 Task Force
Annex B, 15		September 1999	ACP 133 Task Force
Annex B, 40 a		September 1999	ACP 133 Task Force
Annex B, 45		September 1999	ACP 133 Task Force
Annex B, renumbered 46 -132		September 1999	ACP 133 Task Force
Annex B, 47		September 1999	ACP 133 Task Force
Annex B, 52 a		September 1999	ACP 133 Task Force
Annex B, 54		September 1999	ACP 133 Task Force
Annex B, 84		September 1999	ACP 133 Task Force
Annex B, 86 a		September 1999	ACP 133 Task Force
Annex B, 93 a		September 1999	ACP 133 Task Force
Annex B, 133		September 1999	ACP 133 Task Force
Renumber 134 - 201		September 1999	ACP 133 Task Force
Annex B, 160 a		September 1999	ACP 133 Task Force
Annex B, 181 a		September 1999	ACP 133 Task Force
Annex B, 187 b		September 1999	ACP 133 Task Force
Annex B, 187, renumbered c - f		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Annex B, 190 b (3)		September 1999	ACP 133 Task Force
Annex B, 197		September 1999	ACP 133 Task Force
Annex B, 197, module name and oid		September 1999	ACP 133 Task Force
Annex B, 197, Imports		September 1999	ACP 133 Task Force
Annex B, 197 a, c, d, h, i, k, l, m, n, o, s, t, w, x, y		September 1999	ACP 133 Task Force
Annex B, 199, module name and oid		September 1999	ACP 133 Task Force
Annex B, 199, Imports		September 1999	ACP 133 Task Force
Annex B, 199 a (9), (15)		September 1999	ACP 133 Task Force
Annex B, 199 a, renumbered (10) - (14), (16) - (21)		September 1999	ACP 133 Task Force
Annex B, 199 b (7)		September 1999	ACP 133 Task Force
Annex B, 199 b, renumbered (8)		September 1999	ACP 133 Task Force
Annex B, 199 c (66)		September 1999	ACP 133 Task Force
Annex B, 199 c, renumbered (67) - (92)		September 1999	ACP 133 Task Force
Annex B, 199 c (84)		September 1999	ACP 133 Task Force
Annex B, 199 e (11), (24)		September 1999	ACP 133 Task Force
Annex B, 199 e, renumbered (12) - (23), (25) - (30)		September 1999	ACP 133 Task Force
Annex B, 199 g		September 1999	ACP 133 Task Force
Annex B, 201, module name and oid		September 1999	ACP 133 Task Force
Annex B, 201 b		September 1999	ACP 133 Task Force
Annex B, 201, renumbered c - f		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Tables B-25, B-31, B-47		September 1999	ACP 133 Task Force
Renumbered Tables B-26 to B-30, B-32 to B-42, B-45, B-48, B-50to B-52		September 1999	ACP 133 Task Force
Table B-38		September 1999	ACP 133 Task Force
Table B-43, Table B-44		September 1999	ACP 133 Task Force
Table B-49		September 1999	ACP 133 Task Force
Figure B-1		September 1999	ACP 133 Task Force
Figure B-2		September 1999	ACP 133 Task Force
Annex D, 3 i		September 1999	ACP 133 Task Force
Annex D, 3, renumber j - n		September 1999	ACP 133 Task Force
Annex D, 3 j, k, l, m, n,		September 1999	ACP 133 Task Force
Annex D, 4 a (2), (3), (4), (5), (6), (7), (8), (9), (10), (11), (12)		September 1999	ACP 133 Task Force
Annex D, 4 b (2), (3), (4), (5), (6), (7), (8),(9)		September 1999	ACP 133 Task Force
Annex D, 4 c (2), (3), (5), (7)		September 1999	ACP 133 Task Force
Annex D, 4 d (2), (3), (6)		September 1999	ACP 133 Task Force
Annex D, 5 a, b, c		September 1999	ACP 133 Task Force
Annex D, 6 a, b, c, d, e, f, g, h, i, j, k, l		September 1999	ACP 133 Task Force
Annex D, 7 a, b, c, d, e, f, g		September 1999	ACP 133 Task Force
Annex D, 8		September 1999	ACP 133 Task Force
Annex D, 9		September 1999	ACP 133 Task Force
Annex D, 10		September 1999	ACP 133 Task Force
Table D-7		September 1999	ACP 133 Task Force
Table D-9		September 1999	ACP 133 Task Force
Table D-11		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Table D-12		September 1999	ACP 133 Task Force
Renumber Tables D-13 to D-17		September 1999	ACP 133 Task Force
Table D-14		September 1999	ACP 133 Task Force
Table D-16		September 1999	ACP 133 Task Force
Table D-18		September 1999	ACP 133 Task Force
Table D-19		September 1999	ACP 133 Task Force
Table D-20		September 1999	ACP 133 Task Force
Table D-21		September 1999	ACP 133 Task Force
Table D-22		September 1999	ACP 133 Task Force
Table D-23		September 1999	ACP 133 Task Force
Table D-24		September 1999	ACP 133 Task Force
Table D-25		September 1999	ACP 133 Task Force
Table D-26		September 1999	ACP 133 Task Force
Renumber Tables D-27 to D-30		September 1999	ACP 133 Task Force
Table D-30		September 1999	ACP 133 Task Force
Table D-31		September 1999	ACP 133 Task Force
Table D-32		September 1999	ACP 133 Task Force
Table D-33		September 1999	ACP 133 Task Force
Table D-34		September 1999	ACP 133 Task Force
Table D-35		September 1999	ACP 133 Task Force
Renumber Tables D-36 to D-50		September 1999	ACP 133 Task Force
Table D-46		September 1999	ACP 133 Task Force
Table D-53		September 1999	ACP 133 Task Force
Table D-54		September 1999	ACP 133 Task Force
Table D-55		September 1999	ACP 133 Task Force
Table D-56		September 1999	ACP 133 Task Force
Table D-57		September 1999	ACP 133 Task Force
Table D-58		September 1999	ACP 133 Task Force
Table D-59		September 1999	ACP 133 Task Force
Table D-60		September 1999	ACP 133 Task Force
Table D-61		September 1999	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Table D-62		September 1999	ACP 133 Task Force
Table D-63		September 1999	ACP 133 Task Force
Table D-64		September 1999	ACP 133 Task Force
Table D-65		September 1999	ACP 133 Task Force
Table D-66		September 1999	ACP 133 Task Force
Annex D, Appendix 1		September 1999	ACP 133 Task Force
Annex G		September 1999	ACP 133 Task Force
Title Page, Headers, & Footers		March 2000	ACP 133 Task Force
101 e		March 2000	ACP 133 Task Force
211 b		March 2000	ACP 133 Task Force
301 a (1) & (2)		March 2000	ACP 133 Task Force
303 j (1) (b)		March 2000	ACP 133 Task Force
305		March 2000	ACP 133 Task Force
307 a & b		March 2000	ACP 133 Task Force
Figures 3-4 to 3-6		March 2000	ACP 133 Task Force
309 f, g, h, & i		March 2000	ACP 133 Task Force
Insert new 309 i and renumber next subparagraph.		March 2000	ACP 133 Task Force
310 e, f, h, i, j, k, l, p, q, & r		March 2000	ACP 133 Task Force
311 a, m, & p		March 2000	ACP 133 Task Force
Insert new 311 d and renumber subsequent subparagraphs.		March 2000	ACP 133 Task Force
Tables 3-1 to 3-21		March 2000	ACP 133 Task Force
Annex A 5 b		March 2000	ACP 133 Task Force
Annex B 1 a		March 2000	ACP 133 Task Force
Annex B 3 e, n, o, p, & q		March 2000	ACP 133 Task Force
Annex B 4 c		March 2000	ACP 133 Task Force
Annex B 5 a, l, m, r, s, & t		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Insert new 5 c, d, & i into Annex B and renumber subsequent subparagraphs.		March 2000	ACP 133 Task Force
Insert new Table B-17, Table B-18 & Table B-23 and renumber subsequent tables (throughout Annex B). Also, correct references to tables.		March 2000	ACP 133 Task Force
Table B-41 (new #)		March 2000	ACP 133 Task Force
Annex B 7 and 7 e, k, & o		March 2000	ACP 133 Task Force
Annex B 8 d		March 2000	ACP 133 Task Force
Annex B 9		March 2000	ACP 133 Task Force
Annex B 11 a, e, &f		March 2000	ACP 133 Task Force
Table B-54		March 2000	ACP 133 Task Force
Annex B 12 d (3), g, j (1), w, x, y, z, aa, cc, dd (3), ee, ff (3), ii, kk, & mm (1)		March 2000	ACP 133 Task Force
Insert a new subparagraph 12 m into Annex B and renumber subsequent subparagraphs		March 2000	ACP 133 Task Force
Figure B-1 and Figure B-2		March 2000	ACP 133 Task Force
Annex B 16 a and add 16 b		March 2000	ACP 133 Task Force
Annex B 19 b		March 2000	ACP 133 Task Force
Annex B 23 a		March 2000	ACP 133 Task Force
37 a		March 2000	ACP 133 Task Force
40 a		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
41 a		March 2000	ACP 133 Task Force
59 a		March 2000	ACP 133 Task Force
84 b		March 2000	ACP 133 Task Force
94 a		March 2000	ACP 133 Task Force
103 a		March 2000	ACP 133 Task Force
117 a		March 2000	ACP 133 Task Force
120 a		March 2000	ACP 133 Task Force
121 b		March 2000	ACP 133 Task Force
124 a		March 2000	ACP 133 Task Force
160 a		March 2000	ACP 133 Task Force
196 a		March 2000	ACP 133 Task Force
197, 197 k, l, m, n, u, & v		March 2000	ACP 133 Task Force
199 c 75, 85, 90, & 92		March 2000	ACP 133 Task Force
199 f, g		March 2000	ACP 133 Task Force
Insert new paragraphs 21, 22, 23, 28, 57, 70, 176, 184, 197 o, 199 a (1) (2), & (7); 199 c (4), (5), (11), (29), (36), (91) & (93); 199 e (1), (2), & (8) into Annex B and renumber subsequent paragraphs.		March 2000	ACP 133 Task Force
Annex D Table of Contents added		March 2000	ACP 133 Task Force
Annex D 1 a		March 2000	ACP 133 Task Force
Table D-7		March 2000	ACP 133 Task Force
Table D-19		March 2000	ACP 133 Task Force
Table D-21		March 2000	ACP 133 Task Force
Table D-30		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		
Insert a new level of subparagraphs (a - d) below Annex D 6 and renumber existing subparagraphs at the next lower level.		March 2000	ACP 133 Task Force
Table D-42		March 2000	ACP 133 Task Force
Table D-43		March 2000	ACP 133 Task Force
Table D-45		March 2000	ACP 133 Task Force
Table D-49		March 2000	ACP 133 Task Force
Table D-51		March 2000	ACP 133 Task Force
Table D-61		March 2000	ACP 133 Task Force
Insert a new Table D-44 and subparagraph 6 a (4) into Annex D. Renumber subsequent tables and correct references to tables.		March 2000	ACP 133 Task Force
Annex G		March 2000	ACP 133 Task Force

RECORD OF CHANGES AND CORRECTIONS

Enter Change or Correction in Appropriate Column

Identification of Change or Correction; Reg. No. (if any) and date of same		Date Entered	By whom entered (Signature; rank, grade, or rate; name of command)
Change	Correction		

RECORD OF PAGES CHECKED*

Date Checked	By Whom Checked (Signature and Rank)	Date Checked	By Whom Checked (Signature and Rank)

*THIS PAGE NOT APPLICABLE TO US HOLDERS

NOTE: To meet local requirements, this page may be replaced when all entries are filled. The publication holder is to arrange local reproduction, and certify the replacement pages as a “true copy”. The original page numbers are to be allocated to the copy. Superseded pages should then be destroyed in accordance with applicable National instructions.

RECORD OF PAGES CHECKED*

Date Checked	By Whom Checked (Signature and Rank)	Date Checked	By Whom Checked (Signature and Rank)

*THIS PAGE NOT APPLICABLE TO US HOLDERS

NOTE: To meet local requirements, this page may be replaced when all entries are filled. The publication holder is to arrange local reproduction, and certify the replacement pages as a “true copy”. The original page numbers are to be allocated to the copy. Superseded pages should then be destroyed in accordance with applicable National instructions.

TABLE OF CONTENTS

SECTION III

DIRECTORY INFORMATION BASE

SECTION IV

COMPONENTS

SECTION V

PROTOCOLS

SECTION VI

SECURITY OF DIRECTORY

SECTION VII

MANAGEMENT OF DIRECTORY

CHAPTER 3

DIRECTORY INFORMATION

POLICIES AND PROCEDURES

SECTION I

SCHEMA DEFINITION

SECTION II

ENTRY AND ATTRIBUTE POPULATION AND USAGE

SECTION III

REGISTRATION

SECTION IV

SHADOWING

SECTION V

DIRECTORY SYSTEM PERFORMANCE

SECTION VI

CHAINING

CHAPTER 4

DIRECTORY SECURITY POLICES AND PROCEDURES

SECTION I

SECURITY

SECTION II

ACCOUNTABILITY/AUDITING

CHAPTER 5

DIRECTORY MANAGEMENT POLICIES AND PROCEDURES

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

101. General and Scope

a. The function of this document, Allied Communication Publication (ACP) 133, is to define the Directory services, architecture, protocols, schema, policies, and procedures to support Allied communications, including Military Message Handling System (MMHS) services based on ACP 123, in both the strategic and tactical environments. The Directory services are based on the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.500 Series of Recommendations and the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 9594. The Directory specifications will be referred to as X.500 in this document. Note that familiarity with X.500 is assumed.

b. The Allied Directory Services defined in this document are based on the 1993/1995 edition of the X.500 Directory and selected 1997 enhancements. It is expected that an evolutionary period will be necessary for existing directory services to become ACP 133-compliant. In this sense, ACP 133 is viewed as a “target”. The manner, means, and duration of such evolution are outside the scope of ACP 133.

c. This ACP applies to communication among the Allied Directory domains and within a domain for combined operations. It defines a common Directory schema which shall be supported by all Allies for international and combined operations and also records nationally unique attributes to avoid duplicate definitions of elements. It offers support for Internet mail users and transitional support for ACP 127/Joint Army, Navy, Air Force Procedure (JANAP) 128. The Directory has the potential to support different views of directory information such as white pages and yellow pages services.

d. Local interfaces and requirements, such as the specifics of terminal display and local caching, are part of this publication where required to ensure interoperability. ACP 133 includes requirements for which directory information must be displayed to the user, but the format of the display is outside the scope of this document.

e. This third version of ACP 133 defines the services, schema, and protocols required of X.500 Directory System Agents (DSAs) and Directory User Agents (DUAs) to support electronic mail (e-mail), S/MIME, Message Handling System (MHS), MMHS, ACP 127 interworking, and traditional communications. It also identifies security mechanisms that meet the security requirements for strong authentication, confidentiality, integrity, availability, and privilege/label management. As national systems and products mature, this document will be expanded to include more procedural guidance for managing the directory, support for other applications, and additional guidance for operation of tactical (mobile) directories.

102. Background

a. This ACP was written and coordinated by the Combined Communications Electronics Board (CCEB) with the Allied Message Handling (AMH) International Subject Matter Experts (ISME) working group. This group was organized to develop a common messaging strategy that can be deployed to facilitate interoperability among the Allies for military message traffic. Part of this task, and the subject of this ACP 133, was to develop a directory service that could provide access to information needed to do messaging. An ACP 133 Task Force was formed to develop Directory requirements and this ACP.

b. To ensure interoperability with North Atlantic Treaty Organization (NATO) members, ACP 133 was developed in coordination with the NATO Tri-Service Group of Communications and Electronics (TSGCE). TSGCE SC/9 is responsible for developing NATO Standardization Agreements (STANAGs) on data distribution. Rather than developing a separate NATO document, the intention is for this document to satisfy the requirements for military messaging with NATO and United Nations forces.

103. Evolution

This ACP is based on civilian international standards in order to take advantage of the availability of commercial off-the-shelf (COTS) products. As a result, the AMH ISME should monitor the future developments of the international standards and the resultant products. As new capabilities are standardized, those that are found to be useful and appropriate should be added to ACP 133. In order to maintain consistent directory service among the Allies, new versions of this ACP will be developed with formal review and coordination.

104. Overview

a. The Allied Directory is the combination of the parts of the national directories and those Combined Task Force (CTF) directories, when they exist, that are to be shared with the Allies. For example, specific unique directory requirements must be satisfied to support operations which would result from dynamic military operations. Thus, it is envisioned that the Allied Directory will consist of relatively stable shared national and combined domains, as well as, periodic dynamic combined domains to satisfy specific operations involving coalitions of national military forces and organizations, such as NATO. An overview of the Allied Directory is shown in Figure 1-1.

b. The information accessible using the Allied Directory System is contained in the Allied Directory Information Base (DIB). The information published in the Allied Directory DIB is provided to support Allied communications, including MMHS services based on ACP 123, in both the strategic and tactical environments. Besides the information used by the messaging application, the Allied Directory System supports the storage of certificates needed for secure messaging (e.g., ACP 120) and for other secure applications such as Electronic Data Interchange (EDI). The Allied Directory DIB also contains information for managing the components of the Allied communications system.

c. A Directory Management Domain (DMD) is composed of all of the directory components, policies, and information of an organization for the purposes of management. In the Allied Directory System there are two types of directory domains, as illustrated in Figure 1-1: national domains and CTF domains. The union of all national information shared is said to comprise a single logical DIB. A national domain includes the information, policy, and components needed to govern a specific nation's directory services.

d. A CTF domain is a subset of the Allied Directory that is provided by two or more Allies and includes unique mission-related information, policy, and components. The combined domain is owned, operated, and administered by a multi-national military unit. The commander of the CTF establishes the rules and procedures for its domain. No information and components are supplied or maintained by the CCEB. Rather, this ACP defines mechanisms for sharing information and interconnection of national assets to support combined operations. Note that, in this ACP, the significance of the term "combined task force" is very broad and should not be confused with specific "task force" designations already in use by various organizations such as Naval Task Force, defined by AUSCANZUKUS.

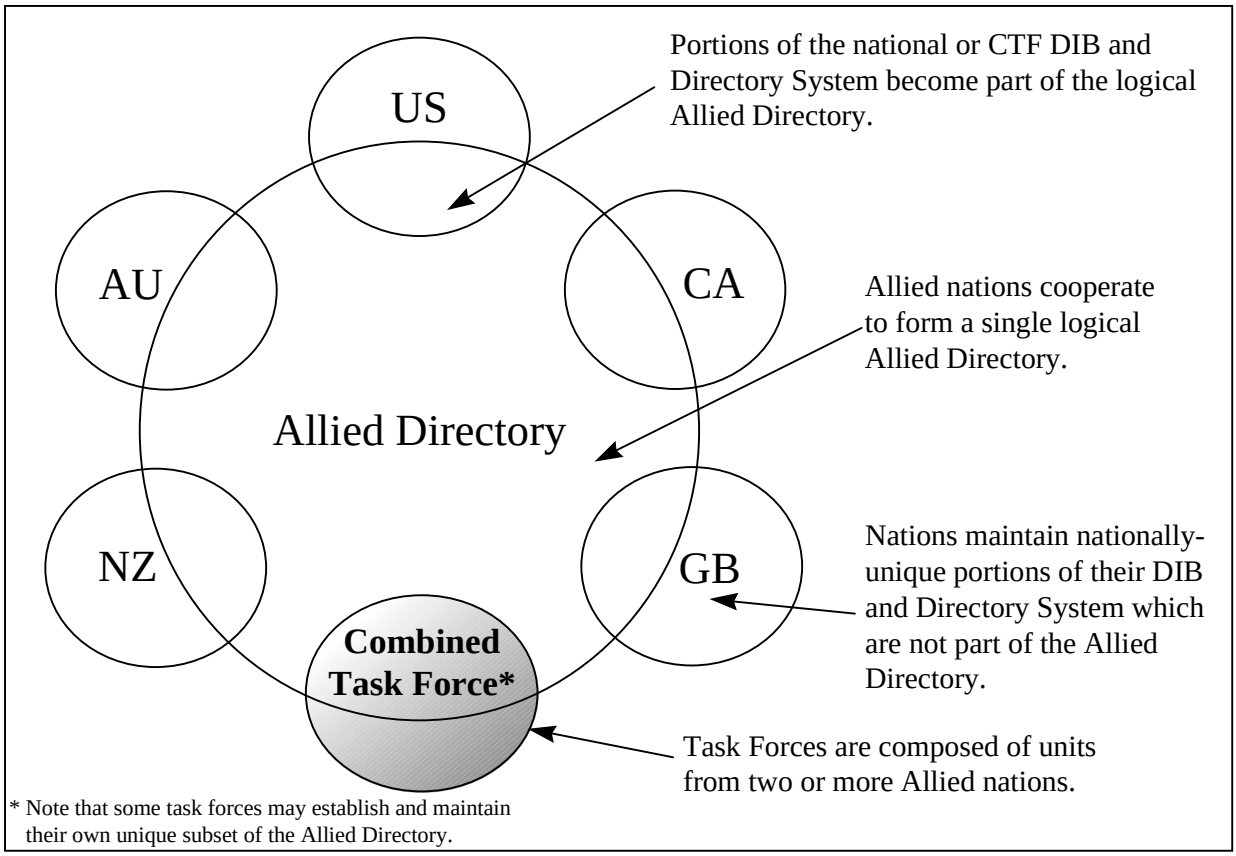

Figure 1-1
Overview of the Allied Directory

e. The X.500 Directory is composed of one or more DSAs that are the repositories for some portion of the DIB. The DIB contains user information and operational information for use by the Directory system. Each user of the Directory, whether a person or an application, uses a DUA to access the Directory. The Directory schema contains the rules governing the contents of the DIB.

f. DUAs and DSAs communicate with each other by using the Directory Access Protocol (DAP). DSAs communicate with each other using the Directory System Protocol (DSP), the Directory Information Shadowing Protocol (DISP), or the Directory Operational Binding Management Protocol (DOP). DSP is used by DSAs to "chain" requests from users when the originating or "home" DSA of the user does not have the requested information. DISP is used in the process of replicating information among DSAs. DOP is used to perform the management aspects of replication necessary for DISP and to maintain the knowledge and access control, collective attributes, and other administrative information. These components and protocols are pictured in Figure 1-2.

g. The logical arrangement of the structure of the DIB is called the Directory Information Tree (DIT). Different parts of the DIT will be managed by different organizations. To accomplish this, the DIT can be divided into subtrees called administrative areas. Policies concerning access control, schema, and collective attributes, which are explained later in this document, may then be formulated for particular subtrees.

h. The Allied Directory schema contains the rules governing the contents of the DIB. The schema includes a set of definitions for Name Forms, DIT Structure Rules, DIT Content Rules, Object Classes, Attribute Types, and Matching Rules. The Allied Directory Schema is based to the extent possible on definitions in the ITU-T X.400 and X.500 Series of Recommendations and other applicable standards for name forms, object classes, attribute types, and matching rules. Where necessary, ACP 133 defines these elements or imports definitions from other sources.

i. In addition to the user information which is controlled by the Allied Directory Schema, the Allied Directory System contains directory administrative and operational information. This system information is governed by the Allied Directory System Schema which is a set of definitions and constraints concerning the information that the Allied Directory System itself needs to know in order to operate correctly. This information is specified in terms of subentries and operational attributes. Subentries contain information relevant to a particular subtree of the DIT, and contain operational attributes. Also, user entries may contain operational attributes, such as, the last time the entry was modified.

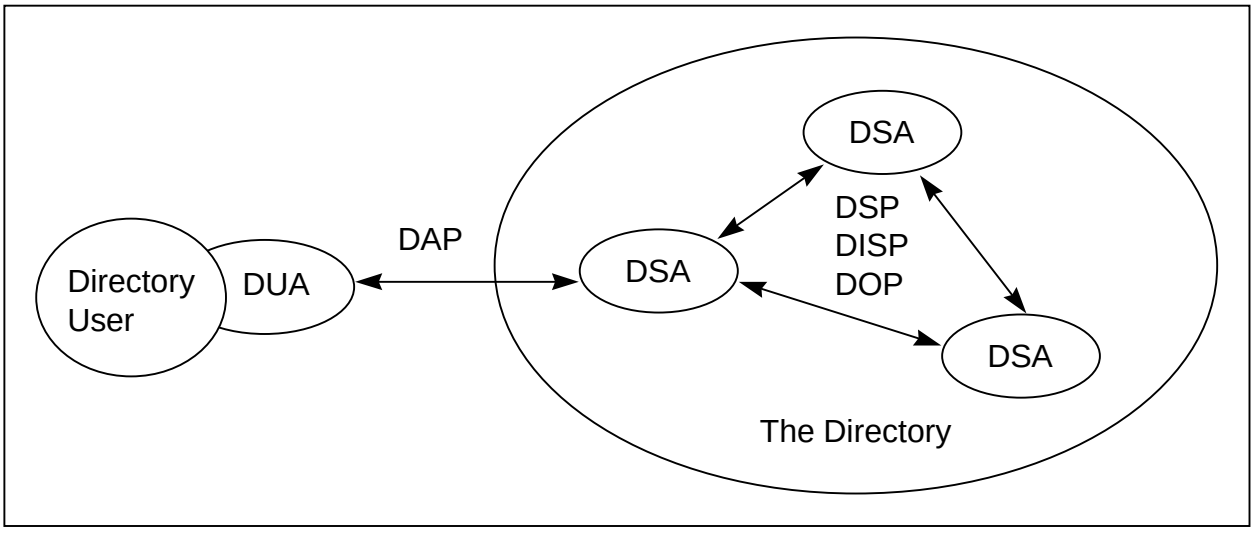

Figure 1-2
The Directory Model

105. Definitions

a. Address List - An Address List is a shorthand method for addressing a predetermined list of recipients.

b. Administrative DUA - An Administrative DUA (ADUA) is a DUA which is used by managers and administrators to query and modify user and system information in the Directory in order to manage the service and administer the information in the DIB.

c. Allied Directory Service - The Allied Directory Service is a capability provided to allied forces to support a variety of information exchange requirements. This service is implemented by the interconnection of national and CTF directory system assets which conform to this ACP.

d. Allied Directory System - The Allied Directory System consists of the components, protocols, administrators, and information that provide the Allied Directory Service.

e. Border DSA - A Border DSA is a DSA that has been designated by a DMD to provide the primary international interface for a nation's or a CTF's Directory System to the rest of the Allied Directory System.

f. Combined Task Force - A CTF is a coalition of forces contributed by two or more nations for a specific operation and period of time.

g. Common Content - The Common Content is the collection of definitions and rules about the Allied Directory System contents. It is the Allied Directory System's Directory Schema.

h. Interrogation DUA - An interrogation DUA uses the read, compare, abandon, list and search operations to query user information.

i. Interrogation/Modification DUA - An interrogation/modification DUA uses all of the Directory Services to query and modify user information.

j. National DSA - A National DSA is an "internal" DSA in a national or CTF DMD that interfaces to the Allied Directory System through a Border DSA.

k. Plain Language Address - A Plain Language Address (PLA) is an abbreviated or non-abbreviated activity (organization) title with its associated geographical location.

l. Population - Population refers to the directory entries and attributes for which values have been entered in the Allied Directory.

m. Schema Support - Support for a schema element means that it can be generated, processed, and displayed in accordance with its definition.

CHAPTER 2

SYSTEM ARCHITECTURE

SECTION I

DIRECTORY SYSTEM

201. General

The Allied Directory is a set of interconnected systems supporting subsets of the total information base. The information that is accessible by users of the Allied Directory is the same for each user, subject to access controls; that is, the Allied Directory service has the appearance of a single information base. The Allied Directory system comprises:

- the services offered to the user
- the information supplied by each Ally
- the systems in which the information is housed or used, i.e., components
- the protocols necessary for exchange of the information among the components
- the means of protecting the information and components against a variety of threats
- the means of managing the information and components.

SECTION II

USER SERVICES

202. User Access to the Directory

a. ACP 123 defines message handling services offered to the user in terms of Elements of Service (EoS) according to the definitions in the X.400 Recommendations. The X.500 Recommendations do not define services offered to the users in this way. In this document, the services that are offered to the Directory user are referred to by the term “user services”. Some user services are described as optional, that is, they are available to the user only if they are offered by the Allied Directory System. The user shall be able to select the appropriate user services for interrogation, modification, and administration of the Allied Directory.

b. Generally, the user services are employed to deal with “directory user information”, that is, the information in the directory about the entities represented by the entries. Administration is a special case of directory usage where access is also necessary to the “directory system information”, which is the information in the entries and subentries concerning the operation of the Directory itself, such as Access Control Information (ACI).

Interrogation, modification, and administration usages of the directory are illustrated in Figure 2-1. Although the figure shows human users, a directory user may be an application process, such as, an MMHS User Agent (UA).

c. The Allied Directory System provides all of the standard X.500 directory user services, which correspond to the formal operations specified for access to a directory system However, the Allied Directory System limits the use of some services by some users. For example, only authorized personnel are allowed to employ the user services that create new entries in the Allied Directory.

d. User authentication is also required by the Allied Directory Service, but in a local environment, this will be defined by national policy. Additional authentication requirements and details are addressed in paragraph 402.

e. For every user service, the results or errors from each request shall be displayed, if the user is a human.

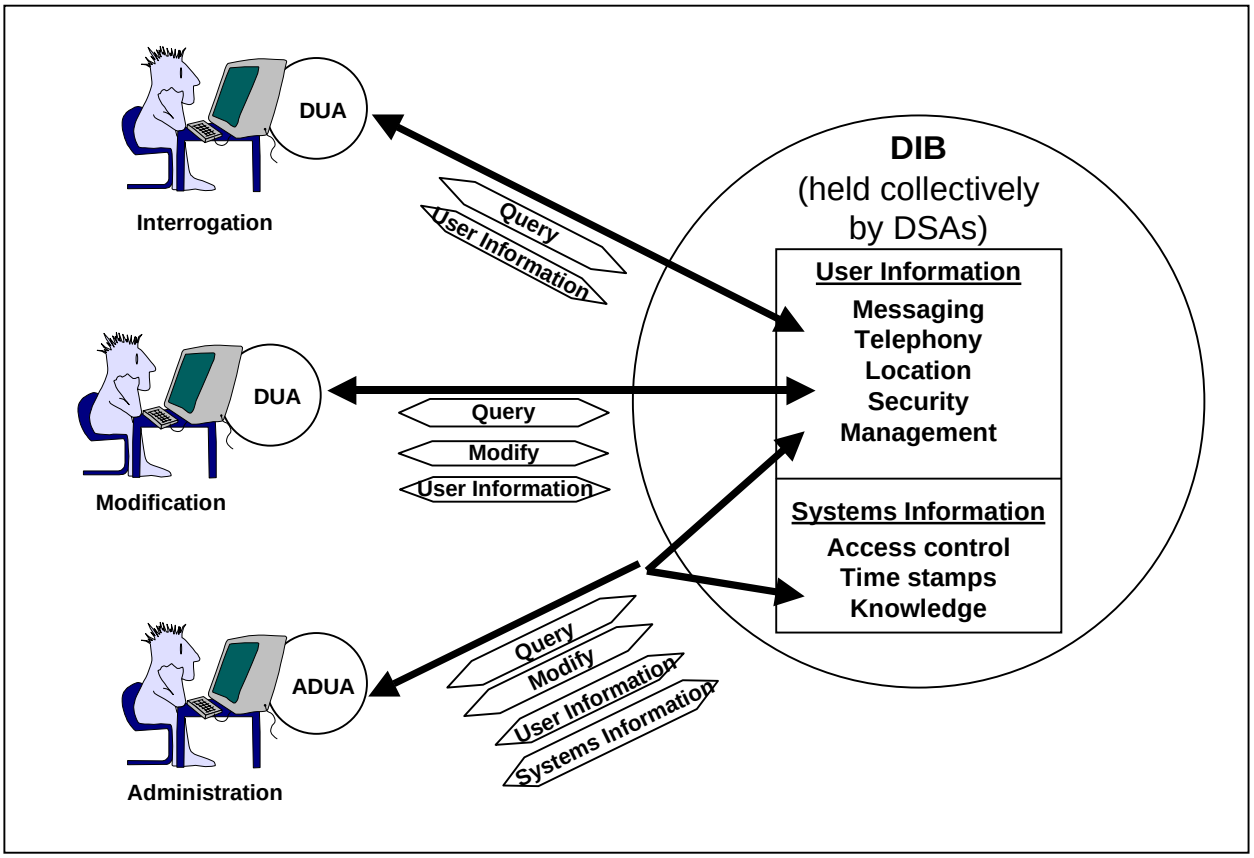

Figure 2-1
Directory User Access

203. Service Parameters and Constraints

The user services provided by the directory system can be parameterized or can be constrained by employing security parameters, by permitting filtering, and by applying entry selection criteria. In order to provide data integrity and data origin authentication, the ability to digitally sign an operation request shall be supported by the Allied Directory System. Likewise, the ability to employ the filter service constraint shall be supported.

204. Common Arguments

a. Each of the directory user services includes arguments specific to the operation being invoked. In addition, there are Common Arguments that may be used to qualify any operation, including Critical Extensions (see paragraph 205), Service Controls (see paragraph 206), and the Requestor Distinguished Name.

b. The Requestor Distinguished Name component of the common argument shall be supplied to all DSAs when records management or logging is required of DSA services or source Distinguished Name (DN) verification is performed by the DSA.

205. Critical Extensions

a. In the critical extensions component of the common argument for an operation, any enhancements that are part of the operation have the corresponding extensions listed. The requirements for the Allied Directory to support critical extensions are as follows. Also, see paragraph 219.

(1) Subentries extension shall be supported for directory administrators.

(2) Copy Shall Do extension is optional.

(3) Attribute Size Limit extension is optional.

(4) Extra Attributes extension shall be supported for Allied Directory administrators.

(5) Modify Rights Request extension shall be supported for Allied Directory administrators.

(6) Paged Results Request extension is optional. This extension shall not be used if results are to be signed.

(7) Matched Values Only extension is optional.

(8) Extended Filter extension is optional.

(9) Target System extension is optional.

(10)Use Alias On Update extension shall be supported for those Allied Directory users that require directory modification user services.

(11)New Superior extension shall be supported for Allied Directory administrators.

b. The following extensions specified in X.511 ’97 edition shall be supported for Allied Directory administrators:

(1) For DAP, DSP, and DISP, signed response for those operations which in X.500 ’97 returned a Null result (e.g., DAP operations Add Entry, Remove Entry, Modify Entry, Modify DN and all DISP operations)

(2) Signed errors

(3) The extensions for security parameters:

- operationCode
  (Note: a defect in the syntax for operation code is being reported.)

- errorCode
  (Note: errorCode is added to security parameters in a defect being reported.)

- procedures for setting the random value in operation result/error

206. Service Controls

a. The Service Controls component of the Common Arguments contains controls that direct or constrain the provision of the directory user services. For example, the priority of the request can be set, or time and/or size limits can be set on the operation responses. Allied Directory support for Service Controls is as follows.

(1) PreferChaining is optional.

(2) ChainingProhibited is optional.

(3) LocalScope is optional.

(4) DontUseCopy is optional.

(5) DontDereference Aliases shall be supported.

(6) Subentries shall be supported for Allied Directory administrators and is optional for other Allied Directory users.

(7) CopyShallDo is optional.

(8) Priority shall be supported. In an ACP 123 environment, this service control shall follow the Grade of Delivery EoS for which the messaging request is made. That is, for directory operation requests that are part of processing a message, the Messaging Grade of Delivery EoS Non-urgent should map to the Directory low priority, Normal should map to medium, and Urgent should map to high. Note that this is not a guaranteed service in that the Directory as a whole,

does not implement priority queuing. There is no relationship implied with the use of priorities in underlying layers.

(9) Time Limit is optional. It shall be monitored by the DSA and have configurable pre-set values to ensure the Allied Directory System is not compromised. Since this service control is dependent on a number of factors, including synchronization between DSA clocks, it is recommended that the abandon user service be used to abort operations which are not completed in the required period of time.

(10)Size Limit is optional. It shall be monitored by the DSA and have configurable pre-set values to ensure the Allied Directory System is not compromised.

(11)Scope Of Referral is optional. It shall be monitored by the DSA and have configurable pre-set values to ensure the Allied Directory System is not compromised.

(12)Attribute Size Limit is optional. Its use is a national matter.

b. Certain combinations of Priority, Time Limit, and Size Limit may result in conflicts. For example, a short time limit could conflict with low priority; a high size limit could conflict with a low time limit, etc.

c. The Service Controls component of Common Arguments shall be supported as an essential feature in all Allied Directory DSAs and DUAs. However, its use is mainly associated with distributed directories, directory management, or controlling response requirements.

207. Distributed Directory Service

Many of the service control facilities deal with parts of the distributed directory information model, e.g., DMD definitions, referrals, master/copy entries. These aspects of distributed directories are subject to national and allied operational requirements.

a. Distributed operations control may employ the following service control elements: Prefer Chaining, Chaining Prohibited, Local Scope, and Scope Of Referral.

b. Master/copy entry selection may employ the following service control elements: Dont Use Copy and Copy Shall Do. Their settings will depend on the user requirement to retrieve master or copy information.

c. Request/response characteristics may be controlled using the following service control elements: Priority, Time Limit, Size Limit, and Attribute Size Limit. In the Allied Directory System, these facilities shall be configurable in ADUAs. For other DUAs, priority should default to medium. The default for Time Limit should be 60 seconds. The default for Size Limit should be set to the number of objects that can be contained in 250 kilobytes. (This can be adjusted for the Directory application and nature of the DUA-DSA access link.)

208. Common Results

The Common Results shall be supported. However, its use should be defined with respect to the application's needs.

SECTION III

DIRECTORY INFORMATION BASE

209. Allied Directory Schema

The Allied Directory Schema encompasses the directory entry types, object classes, attributes, matching rules, name forms, and structure rules that are necessary for specifying the information that is stored in the Allied Directory System. Components of the Allied Directory System shall implement all of the standard object classes, attributes, and name forms defined in X.501, X.509, X.520, X.521, and X.402, as profiled in Annex D. The Allied Directory Schema, called Common Content, employs the standard schema elements and also includes object classes, attributes, and name forms defined in this ACP especially to meet Allied requirements. The Allied Directory Schema is specified in Annex B and is profiled in Annex D.

210. Directory Entries for Messaging Users

One purpose of the Allied Directory is to provide access to stored information about organizations and individuals in various Allied domains to enable them to exchange messages, that is, to be users of the message exchange services defined in ACP 123. The stored information is the DIB in which each entry represents a user or group of users. Three types of entries are defined, corresponding to the organizational unit, organizational role, and organizational person (individual) categories of messaging users. A fourth type of entry, address list, is defined for representing groups of users.

211. Content Rules

a. Content rules are used for two purposes in defining Allied Directory entry types.

b. First, a content rule can be used to define one or more entry types with a base structural object class by adding auxiliary object classes and adding (or deleting) attributes without creating a new object class. For example, an MHS Message Store (MS) entry may be defined by specifying the mhs-message-store structural object class, the securePkiUser auxiliary object class, and aliasPointer, effectiveDate, and expirationDate optional attributes in an aCPMhs-message-storeRule content rule. The auxiliary object classes listed in a content rule are not required to be used in every instance of the type of entry specified. Each allowed auxiliary object class that is used in an entry is identified in the value of the entry's objectClass attribute. For example, using the aCPOrganizationalPersonEdBRule content rule defined in Annex B, an entry for every instance of Organizational Person would have to include commonName and surname. If the person does X.400 mail, the object identifier for mhs-user would be added to the

entry, and this would make mhs-or-addresses mandatory and mhs-deliverable-content-types optional. If the person needs a certificate, the object identifier for securePkiUser would be added to the entry, and userCertificate would be allowed. The end result is that the Directory could contain entries for different persons with different mandated attributes. The use of a content rule to define one or more entry types is used extensively in defining the Common Content.

c. Secondly, the directory standard requires the use of a content rule to allow the application of collective attributes to an entry type, since none of the object classes are allowed to contain collective attributes. For example, ACP 133 uses the standard object class for organizational person, in which postal address is an attribute. The local administrator may choose to make the postal address a collective attribute, if that is more efficient than entering a postal address in the entry for every individual at the same location. In this case, a content rule permitting the collective postal attribute would have to be defined and applied. The example content rules given in Annex B would require modification to permit collective attributes in entries.

d. Nations may add nationally-specific attributes to the example rules, given in Annex B; however, this may affect management and interoperability of the directory information in combined environments.

212. Directory Information Tree

Entries in the Allied Directory are arranged in the form of an inverted tree, called the DIT, where the vertices represent the entries. Each entry adds the value of one or more attributes. The ordered list of the values of the branches through the tree to a user entry is the DN for the entry. The entries highest in the Allied Directory tree represent countries and international/multinational organizations (such as NATO), those in the middle represent organizations and localities, and those at the bottom represent individuals, application processes, address lists, etc.

213. Subtrees

a. The Allied Directory DIT is specified by this ACP, with some levels defined by national policy as shown in Figure 2-2 and described here. For each Ally, Country is the initial entry under the root. The definition of the Country entry and the location of the master entry for Country are controlled by the country itself and are outside the scope of this ACP. The Country entry described in Annex B assumes the standard definition from X.521, which is satisfactory for purposes of the Allied Directory. The arrangement of the ally-specified levels of the DIT, the values of the entries, and the location of the master entries are a matter of national policy and are outside the scope of this ACP. However, each of the Allies has provided this information for inclusion in Annex B. Although published here, this ACP is not the official source for this national information.

b. Below the Country entry of an Ally, one of the subtrees includes the armed forces of the Ally, e.g., Department of Defense for the U.S. The armed forces are represented by an

organization or organizational unit. Below the armed forces level each Ally has defined the subtrees that contain the information needed to represent its forces, including Services, agencies, and commands. The commands include the CTFs that are led by the Ally. The armed forces subtrees of each Ally are shown in Annex B.

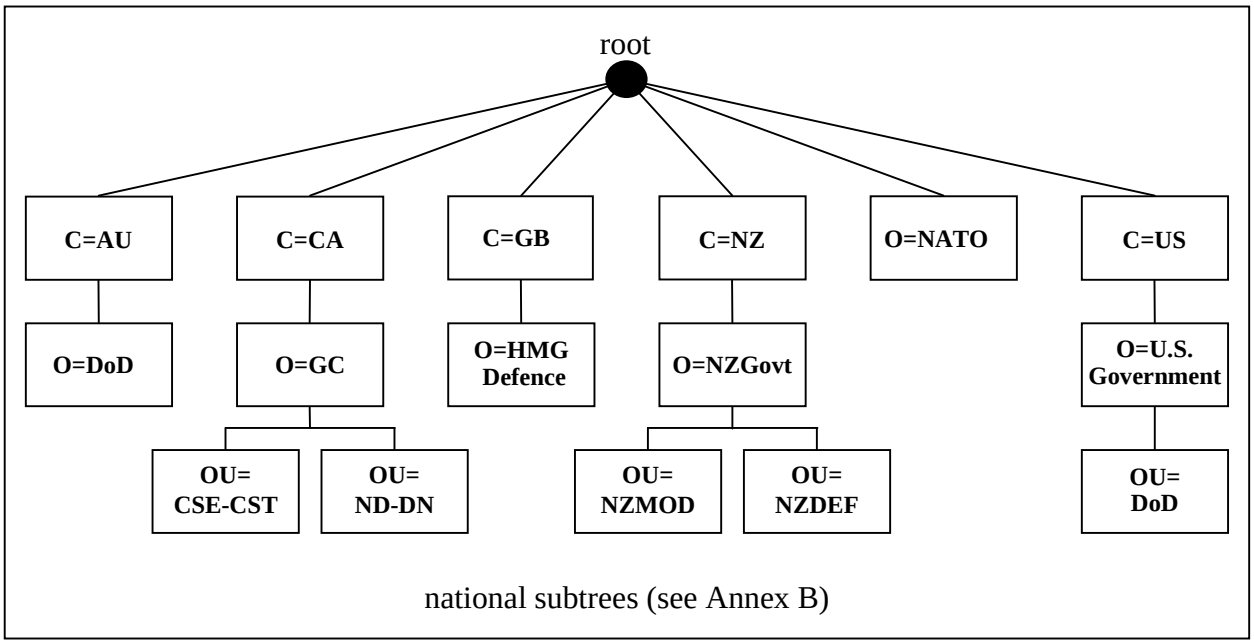

Figure 2-2
Top-Level Allied Directory DIT

SECTION IV

COMPONENTS

214. General

a. The components of the Allied Directory System are: DSAs, Border DSAs, and DUAs. An example of interconnecting these components is illustrated in Figure 2-3.

b. This section applies to both national and combined domains described in paragraph 104. The DSAs within a CTF domain are termed “National” and “Border” in a manner analogous to a national domain. That is, a National DSA in a CTF domain is only connected to DSAs within the domain and connections to other domains are made by Border DSAs.

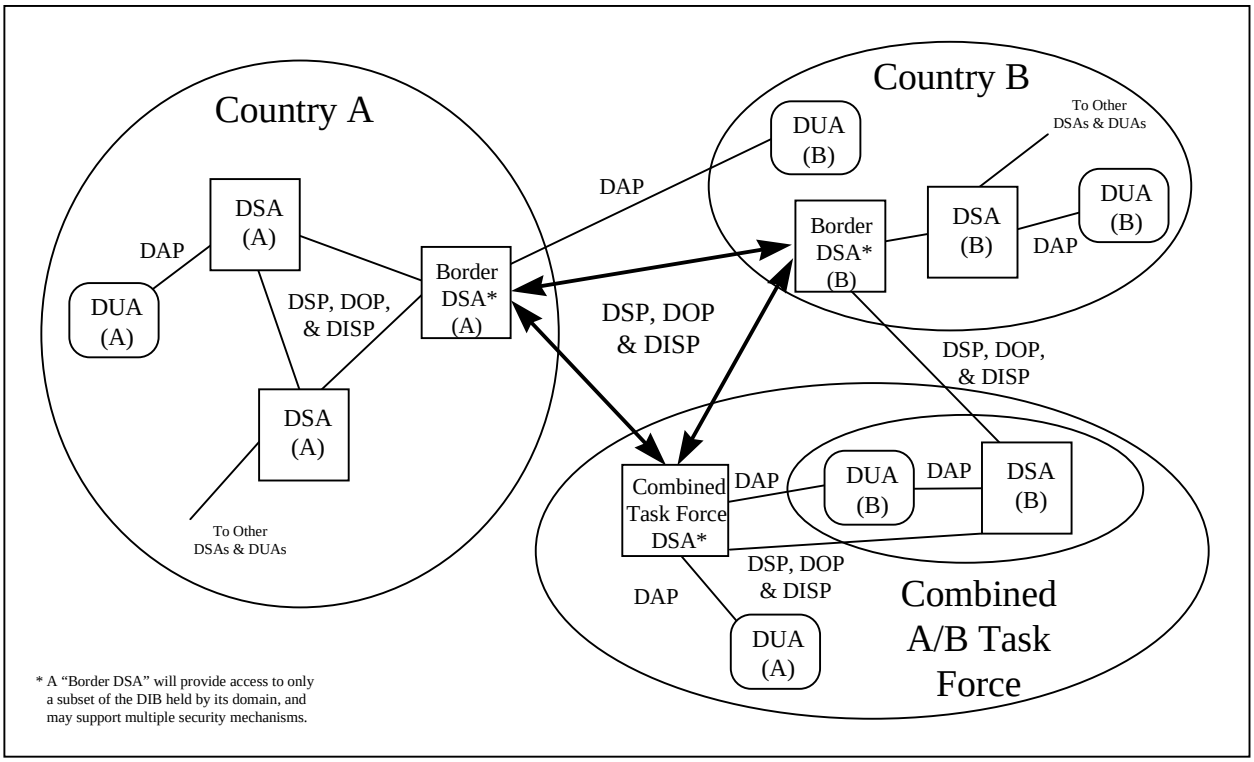

Figure 2-3
Example Allied Directory Configuration

215. DSAs

a. DSAs, collectively, hold the Allied DIB and interact with one another to make the entire DIB accessible to the directory users. The directory system is comprised of DSAs that interact with one another to perform the directory services described above. The DSAs interact with DUAs to get user requests and provide the results from processing the requests.

b. Within each DMD, the distribution of directory information among multiple DSAs is a national/combined task force matter, subject to the quality of service, management, and security provisions of this ACP.

c. The Allied Directory System is composed of a two-tier hierarchy of DSAs: Border DSAs and National DSAs. Both types of DSAs provide functionality as specified in International Standardized Profiles (ISP) 1993 Directory Application Profile (ADY)21, ADY22, ADY42, ADY43, ADY45, 1993 Directory Interchange Format and Representation Profile (FDY)11, and FDY12 with the further requirements defined in Annex D.

d. The contents of National DSAs are a national matter, except that a common definition of National DSA contents is necessary for interoperability of assets from different nations in CTF domains. Note that the contents of the Border DSAs and National DSAs are the information the

ally makes available in the Allied Directory System. Which Services/agencies/commands, entries, or attributes from the national directory service are included in the Allied Directory System is a national or CTF matter. A combination of Directory access controls (and other separation mechanisms) may be used to effect the segregation of domain-specific and shared information.

e. The time limit argument of Chaining Arguments is dependent on synchronization between DSA clocks to an order of magnitude less than the time limit. If such synchronization cannot be achieved, it is recommended that the chained abandon service be used to abort operations which are not completed in the required period of time.

216. Border DSAs

a. A Border DSA is a logical DSA that has been designated to provide the primary international interface for a nation's or CTF's directory system. The implementation of an instance of a Border DSA may be a specific or separate component or a logical partition of the information. Border DSAs are interconnected to enable the sharing of directory information across DMDs. Within a CTF, DSAs from the participating Allies shall interoperate in accordance with this ACP.

b. A Border DSA shall perform many functions that ordinary DSAs within a nation or CTF need not support. One of the major functions of a Border DSA is to provide the portion of the national/task force DIB available for access in the Allied Directory System. Thus, some portions of the national DIB may be unavailable. Also, a different security policy may apply to Border DSAs than national DSAs.

c. The process for resolving directory queries within a particular national directory domain is beyond the scope of ACP 133. Valid options include utilizing a shadow of the national/task force DIB maintained locally within the Border DSA, chaining the query onward into the national/task force domain, or providing a referral to a specific internal DSA that can be accessed by the user. A nation/task force may designate any number of DSAs as Border DSAs.

217. DUAs

a. The directory access facilities required by the Allies dictate that DUA functionality is provided in a number of forms. DUA functionality will be embedded into commercial products which provide the user desktop services as well as providing specific infrastructure functions such as information retrieval for Message Transfer Agents (MTAs).

b. DUAs make requests on behalf of the directory user and present results back to the user. For example, a user can request the Originator/Recipient (O/R) address of a messaging user in another country. DUAs are interconnected with DSAs (including Border DSAs). DUAs provide functionality as specified in ISPs ADY11, ADY12, ADY41, FDY11, and FDY12 with the further requirements defined in Annex D.

c. The degree to which a DUA is integrated with a UA, e.g., a Military Messaging User Agent (MMUA) or Mail List Agent (MLA) or other application that is a directory user, varies

according to the application, its implementation, and the degree of human involvement in directory information access. A DUA may be an entirely independent application.

d. ACP 133 defines three types of DUA functionality. DUAs with different functionality than is defined here may be used as a national option.

(1) An "Interrogation" DUA uses the Read, Compare, List, Search and Abandon services only. This type of DUA enables directory users to request information from entries. These services may be constrained by the limitations of the DUA, and they are limited by the DSA access controls.

(2) An "Interrogation/Modification" DUA uses all of the Directory services. Such a DUA enables directory users to obtain information by directly reading an entry or by locating interesting entries based on their content or partial name as well as modify entries. These services may be constrained by the limitations of the DUA, and they are limited by the DSA access controls.

(3) An "Administrative" DUA uses all of the Directory services. This type of DUA enables a directory user to act as a Directory System Administrator, creating, modifying, and deleting user entries and directory operational information. Access controls will limit what functions of an Administrative DUA may be used by a specific user.

e. Authentication of DUAs is addressed in paragraph 402.

f. A DUA may receive a continuation reference when a DSA responds to an operation by issuing a referral to another DSA. A DUA might also receive a continuation reference as part of an incomplete List or Search result.

(1) Some DUAs may be designed for use in environments where such references are never used, or a DUA may be simplified such that it cannot pursue a reference. Alternatively, a DUA may be designed to be capable of pursuing references. Another possibility is that a DUA product is designed to be configurable such that the capability to pursue references may be controlled (either by the user or by the system administrator). In any case, when a DUA does not automatically pursue a continuation reference, the reference shall be passed to the user so that a procedure can be used instead.

(2) Continuation references received in List or Search operations shall be handled by the receiving DUA (by displaying them, etc.); however, their automatic continuance by the DUA will be subject to national policy. In general, so that search or list loops are deleted, it is preferable that continuation references be performed by DSAs rather than by DUAs.

SECTION V

PROTOCOLS

218. General

a. To ensure interoperability among DUAs and DSAs from different nations, the X.500 standard protocols are used for Allied Directory communications. These protocols are:

- DAP
- DSP
- DISP
- DOP

b. Figure 2-3 shows which protocols apply to each type of interconnection. Use of these protocols is a requirement within a CTF domain. Otherwise, use of these protocols within a national domain is outside the scope of this ACP.

219. DAP

a. DAP is used to convey requests for directory information to a DSA and to return the results to the DUA. DAP is used between a DUA and a Border DSA in different domains and between a DUA and a DSA in a CTF domain. DAP shall be implemented as specified in ISPs ADY11, ADY12, ADY21, ADY41, and ADY42 with the further requirements defined in Annex D.

b. DAP is used to access the Services of the Allied Directory.

(1) Table 2-1 shows the DAP operations that shall be implemented by each type of DUA.

Table 2-1
DAP Operations Implementation

Operation	Interrogation DUA	Interrogation/ Modification DUA	Administrative DUA
bind	m	m	m
unbind	m	m	m
read	m	m	m
compare	m	m	m
abandon	m	m	m
list	m	m	m
search	m	m	m
add entry	o	m	m
remove entry	o	m	m
modify entry	o	m	m
modify DN	o	m	m

(2) DSAs shall implement all DAP operations.

(3) Table 2-2 shows support for Critical Extensions.

Table 2-2
1993 Critical Extensions Support Summary

Extension	Interrogation DUA	Interrogation/ Modification DUA	Administrative DUA	DSA
subentries	o	o	m	m
copyShallDo	o	o	o	m
attributeSizeLimit	o	o	o	o
extraAttributes	o	o	m	m
modifyRightsRequest	o	o	m	m
pagedResultsRequest	o	o	o	o
matchValuesOnly	o	o	o	o
extendedFilter	o	o	o	o
targetSystem	o	o	o	o
useAliasOnUpdate	o	m	m	m
newSuperior	o	o	m	m

Table 2-3
1997 Extensions Support Summary
(see X.511(1997) §7.3.1 Table 1)

Extension	Interrogation DUA	Interrogation/ Modification DUA	Administrative DUA	DSA
manageDSAIT	o	o	o	o
useContexts	o	o	o	o
overspecFilter	o	o	o	o
selectionOnModify	o	o	o	o
Security parameters - response	o	o	o	o
Security parameters - operation code	o	o	m	m
Security parameters - attribute certification path	o	o	o	o
Security parameters - error protection	o	o	o	o
Security parameters - error code	o	o	m	m
SPKM Credentials	o	o	o	o
Bind token - response	o	o	o	o
Bind token - Bind Int. Alg, Bind Int Key, Conf Alg and Conf Key Info	o	o	o	o
Bind token - DIRQOP	o	o	o	o

220. DSP

a. DSP is used to convey an information request to another DSA when the requesting DSA does not have the complete information requested, i.e., to do chaining, and to return the results to the requesting DSA. DSP is used between Border DSAs in different domains and between a DSA/Border DSA and another DSA in a CTF domain. DSP shall be implemented as specified in ISPs ADY22, ADY43, ADY45, and ADY61 with the further requirements defined in Annex D.

b. DSP consists of the operations, results, and errors defined for DAP plus additional information exchanged among the DSAs to notify each other of the progress and results of the operation.

(1) The operations defined in DSP are:

- bind
- unbind
- chained read
- chained compare
- chained abandon
- chained list
- chained search
- chained add entry
- chained remove entry
- chained modify entry
- chained modify DN

(2) Any of the DSP operations can be initiated by any DSA. In particular, the DSA that receives a request from a DUA is responsible for initiating the first chaining operations, when necessary. Then, if further chaining operations are needed, whichever DSA needs more information initiates the next operation.

c. When requested information is not present in the home DSA, chaining is preferred over referral for access to international information. To access information that is specific to country B, a DUA within country A would access the directory through its home DSA. The home DSA would chain the operation to the appropriate Border DSA within country A. Depending on the specific information requested and on the shadowing agreements that are in place, the country A Border DSA may either complete the operation locally or further chain the operation to a country B Border DSA. Similarly, the Border DSA in country B may contain a master or shadow copy of the desired information, or it may chain the request onward within country B. Both chaining and referrals shall be supported in the Allied Directory (see paragraph 323).

d. DSAs shall support in DSP the same critical extensions supported for DAP as shown in Table 2-2.

221. DISP

a. DISP is used to replicate information in the Allied Directory by conveying shadow copies of directory information from one DSA to another as described in paragraph 316. DISP is

used between Border DSAs in different domains and between a DSA/Border DSA and another DSA in a CTF domain. Prior to using DISP, an agreement to shadow is arranged and activated. In the DSA sending the shadow, the information may be the master copy or a shadow copy of the information. Both primary and secondary shadowing shall be supported. DISP shall be implemented as specified in ISPs ADY51, and ADY62 with the further requirements defined in Annex D.

b. The operations defined for performing the replication of the Directory Information are:

- bind
- unbind
- request shadow update
- update shadow
- coordinate shadow update

c. All DSAs that implement shadowing shall implement all of the DISP operations.

d. Which DSA initiates each of the DISP operations depends on which DSA is the consumer and supplier, as arranged in the shadowing agreement.

222. DOP

a. DOP is used to activate, deactivate, and modify shadowing agreements that have been arranged between DSAs and to exchange knowledge and access control, collective attributes, and other administrative information contained in subentries. DOP is used between Border DSAs in different domains and between a DSA/Border DSA and another DSA in a CTF domain. DOP shall be implemented as specified in ISPs ADY71 and ADY72 with the further requirements defined in Annex D.

b. The operations defined for DOP are:

- bind
- unbind
- establish operational binding
- modify operational binding
- terminate operational binding

c. All DSAs that implement shadowing or exchanging knowledge or other administrative information shall implement all of the DOP operations.

d. The DSA that initiates the association is the initiator of the DOP operations performed in the association.

223. Underlying Protocols

All of the Directory protocols include the Association Control Service Element (ACSE) and operate over the Presentation and Session Layer protocols. These protocols are profiled in ISO/IEC ISP 15125-0, Common Upper Layer Requirements (CULR) for the Directory. Below the Session Layer, the directory applications require a connection-oriented transport service that may be provided in a variety of ways, depending on the underlying networks and internetworking environment.

SECTION VI

SECURITY OF DIRECTORY

224. Security Mechanisms

The Directory protocols include security mechanisms that meet the security requirements for the Allied Directory System. Therefore, no additional protocols are employed to protect the Allied Directory System and Services.

SECTION VII

MANAGEMENT OF DIRECTORY

225. Management Architecture

a. Figure 2-4 illustrates a model for systems management interfaces for the Directory. The interfaces that do not indicate a protocol, such as, between a DSA and a management agent, are not standardized.

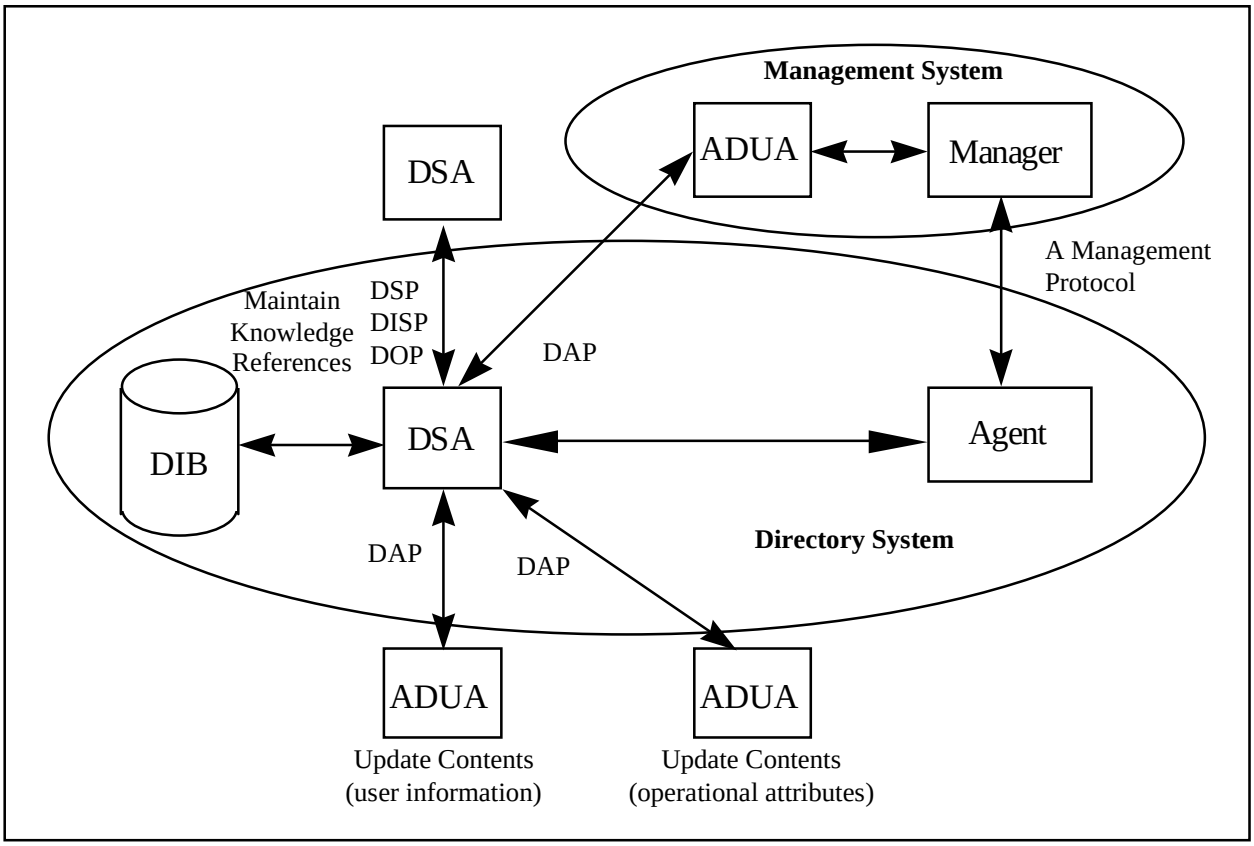

Figure 2-4
Model for Management of the Directory

b. All aspects of management leading to processing, recording, communication and logging of information shall be configurable.

226. Management Protocols

Management protocols, such as Common Management Information Protocol (CMIP) or Simple Network Management Protocol (SNMP), are outside the scope of this ACP.

227. Year 2000 and Date/Time Format

a. Background

(1) The format for date/time in X.500 in some instances is defined as UTCTime. This format is not Y2K compliant because it uses two digits to represent the year. New definitions use GeneralizedTime, which uses four digits to represent the year.

(2) Some of the problems with UTCTime have been corrected by technical corrigenda (TC). TC2 to X.520 amended the UTC Time Match to say that “UTC times with year values 50

to 99 shall be taken to represent times that are earlier than UTC times with year values 00 to 49." TC3 to X.509 replaced UTCTime with Time, which is a choice of UTCTime or GeneralizedTime and gave directions on how to rationalize UTCTime into a four-digit year value.

(3) Both of these corrigenda have been included in the 1997 edition of the Directory specifications, and they are referenced in the latest drafts of the ISPs for the 1993 edition of X.500. A draft TC is being processed to add the choice of UTCTime to the other occurrences of time in X.500. The reason that a choice was added rather than changing occurrences of UTCTime to GeneralizedTime was for backward compatibility. Eventually the use of UTCTime should be phased out.

b. UTCTime

(1) UTCTime values shall be expressed as Greenwich Mean Time (Zulu) and shall include seconds (i.e., times are YYMMDDHHMMSSZ), even where the number of seconds is zero.

(2) To correctly interpret UTCTime past the year 2000 (Y2K) the two-digit year associated with UTCTime shall be rationalized into a four-digit year value as follows:

(3) if the 2 digit value is 00 through 49 inclusive, the value shall have 2000 added to it;

(4) if the 2 digit value is 50 through 99 inclusive, the value shall have 1900 added to it.

(5) In no case shall UTCTime be used for representing dates beyond 2049. Definitions of new schema elements that include time are to be defined as specified in paragraph 302.

c. GeneralizedTime

GeneralizedTime values shall be expressed as Greenwich Mean Time (Zulu) and shall include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero. GeneralizedTime values shall not include fractional seconds.

d. Interworking

The use of GeneralizedTime may prevent interworking with implementations unaware of the possibility of choosing either UTCTime or GeneralizedTime. It is the responsibility of those specifying the ACP 133 domains in which allied systems are interconnected that this specification be used.

e. Certificate Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a

sequence of two dates as defined above: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime.

f. Audit Trails and Engineering Logs

Although it is unlikely that audit trail information and engineering log information from ACP 133 (interworking) systems will be exchanged between allies. It is requested that all the support and management facilities of ACP 133 compliant systems are Y2K compliant. Each nation should request such compliance for these management areas when selecting their products/vendors.

CHAPTER 3

DIRECTORY INFORMATION

POLICIES AND PROCEDURES

SECTION I

SCHEMA DEFINITION

301. Schema

The schema policy for ACP 133 is to support the Allied Directory schema and the Allied Directory system schema as profiled in Annex D using the schema specifications given in Annex B. The Allied Directory schema, which is called the Common Content, includes the specification of user information stored in the Directory. The Directory system schema includes the specification of information that is required to control and manage the DSAs themselves. Support for a schema means that a DUA or DSA shall be able to handle the information types (e.g., object classes, attribute types).

a. Common Content

(1) The Common Content includes object classes, name forms, matching rules, and attributes from the X.500 and X.400 standards, from Request for Comments (RFC) 1274, and those defined in this ACP. The Common Content is summarized in Table B-55. The types of attributes that are present in a directory entry is dependent on the object class or classes to which the entry belongs. ACP 133 specifies the attributes and object classes in the Common Content that must be supported for military applications.

(2) Requirements and guidelines for population of the Common Content for specific applications are found in paragraph 311. A few supplementary attributes, which are not defined as a part of the Common Content, but may be used by two or more nations, are included in Annex B. These are termed “useful attributes”. Useful attributes shall not be replicated, unless specific bi-lateral arrangements are made for their support on both the supplier and consumer systems.

(3) Nations may need to define additional objects and attributes. The schema for the Allied Directory does not preclude such extensions. However, the additional information stored in national extensions might not be accessible as part of Allied Directory Services.

(4) For the interoperation of ACP 127/JANAP 128 systems and ACP 123 systems, provision is made in the Common Content for including information about PLAs.

(5) The Allied Directory System shall enforce the Common Content to ensure that the structure and contents of the DIB remain well-formed over time as modifications are made. Action is taken to prevent the wrong attributes being added for an object, to ensure that the

values are in the correct form for the attribute type, and to ensure that objects are correctly placed in the DIT.

b. Directory System Information

The system schema for the Allied Directory System includes operational attributes such as the time an entry was created, knowledge references, designation of administration points, and ACI. The system schema supported by the Allies is specified in Annex B and profiled in Annex D. The meaning of support for system schema elements is explained in FDY12.

c. Support by DUAs and DSAs

(1) All DSAs and DUAs, including ADUAs, shall support the Common Content in accordance with Annex D. DSAs and ADUAs shall also support the system schema in accordance with Annex D.

(2) Use of MLAs is a national/CTF matter.

(3) Use of MHS distribution lists is a national/CTF matter.

(4) Use of alias pointers is a national/CTF matter.

(5) The application of collective attributes to the DIT is subject to national/CTF policy.

d. Management Information

The Allied Directory System may contain a range of information objects for the purpose of supporting the management of the communications system. This management information is in addition to the management information that supports the management of the directory system itself such as operational attributes, subentries, and knowledge references. These additional management objects provide support for message routing, system functions (such as MTAs and gateways), communications profiles, and logging entities, etc. These objects, where possible, use definitions as specified in the relevant standard (e.g., ISO/IEC 10021-10 and RFCs 1801, 1836, 1837 for X.400 routing and management). Currently, none of these standards is covered by the Common Content.

302. Time Definitions

All new definitions related to time shall use the data type Generalized Time. (Generalized Time uses a four-digit representation of the year of Universal Coordinated Time (UTC) rather than a two-digit representation.)

303. Directory Names

a. Each nation or international organization is responsible for assuring the uniqueness of names in its subtree.

b. The DIT should be organized to keep the number of levels as few as possible and to have no more than ten levels.

c. An individual may have multiple identities. For example, one person may have one identity as an individual and another as a security officer or other role. The person's name would be included in the entry for the role as role occupant. Alternatively, many individuals may support a single role function. The commonName would reflect the role name convention. The seeAlso attribute may be used to cross-reference the entries holding the other identities.

d. Additional values besides the distinguished value may be included in naming attributes. An additional name allows for different values to produce a successful result when searching for an item in the Directory. For example, the commonName attribute could include the Relative Distinguished Name (RDN) value: “Smith, Robert K” plus an additional name: “Bob Smith”.

e. Each entry in the Allied Directory has a unique and globally unambiguous name, the DN, which is composed of the values of the attributes indicated for naming in the DIT. For example, a person’s name could be { C=US, O=U.S. Government, OU=DoD, OU=Navy, OU=locations, L=Washington DC, CN=Jackson, Robert }.

f. The values of attributes composing directory names (i.e., DNs) should be kept as short as possible while remaining meaningful and unique.

g. In order to avoid reassigning users' directory names each time they are promoted, a rank indication shall not be included in the common name distinguished value of the relative RDN attributes of persons. The rank attribute is used for this purpose.

h. When creating a directory name, any appropriate combination of upper and lower case characters may be used in character string values, as directory operations are case insensitive in matching character strings for selecting an entry.

i. For naming an organizational person, this ACP permits the RDN to have multiple components, that is, have a distinguished value in more than one attribute. For example, the RDN could be a distinguished value of commonName plus a distinguished value of organizationalUnitName.

j. Using a DN qualifier as a second component of an RDN to identify an entity in the directory uniquely is permitted for some types of directory entries. For example, the RDN of an Organization entry could be a distinguished value of organizationName plus a distinguished value of dnQualifier.

(1) In order to ensure that these qualifiers are used in an optimal way, the following naming policy is recommended.

(a) Where possible, the RDN should consist of a single component.

(b) Since conflict may arise with some object names, provision is made for the DN Qualifier to be used in addition to the mandatory naming attributes for Organizational Person Ed. A, Organization, Organizational Role Ed. A, Organizational Unit Ed. A, Application Entity Ed. A, Certification Authority Ed. B, Release Authority Person Ed. A and Role Ed. B entries. This DN Qualifier must be locally administered.

(c) In the directory systems that support Certificate Management Infrastructure (CMI) applications, it may be desirable to organize the CA's certificate and user's certificate release information that have common properties into "domains".

(2) This directory organization optimizes the certificate path processing and CA operational management. When organized in such a fashion, CA directory entries require a multi-component RDN. ACP 133 satisfies this requirement by permitting DN Qualifiers in the name forms for organization, organizational unit, organizational role, and application entity object classes.

(3) The use of DN Qualifier in ACP 133 has the semantics of a unique identifier and not the precise meaning as defined in X.520.

k. Although the localityName and stateOrProvinceName attributes are optional in the locality object class in X.521, one or the other of them shall be present in Locality entries in the Allied Directory because they are the naming attributes for localities.

l. The RDN shall not include the full stop character (period), even when an abbreviation is included in the value.

m. The distinguished value of common name of an organizational person shall be in the order: last name, first name, middle initial (s), generation qualifier. Other values of common name may be ordered differently.

n. A directory object may have one or more alias entries that point to the object entry. For example, an EDI party name may be an alias that maps to the Directory name of an organization. Another example is the temporary maintenance of an alias for an individual at one location when he has been transferred to another location.

o. When aliases are used, there is a need to keep them synchronized with the DNs they point to. Standardized management tools will be needed to perform this alias/distinguished name synchronization.

304. Organizational Roles

Provision is made in Common Content for nations to establish directory entries for functional roles in addition to entries for individuals and organizations. These entries will tend to be more stable than those for individuals and may be especially useful for tactical organizations. In addition to a generic organizational role, three roles are recognized in this ACP: Certification Authority (CA), Security Officer, and Release Authority.

305. Certification Authority Function

In the Allied Directory, the CA function may be represented as a special case of an organizational role object. Alternatively, a CA can be represented in the Allied Directory as a special case of any of three other objects: organization, organizational unit, or application entity. In any case, the distinguished value of the commonName, organizationName, or organizationalUnitName attribute of a Certification Authority Ed. B directory entry is a national issue. The naming conventions associated with each nation's CA will be in accordance with each nation's Certificate Policy and Certification Practice Statement (CPS).

306. Security Officer Function

The role of security officer for an organization is represented in the Allied Directory by an Organizational Role directory entry that has, in the commonName attribute, the distinguished value "securityofficer-n", where n is a numeric value. The significance of the number is solely to differentiate the entries and no order or ranking is implied. There are no spaces in the string.

307. Release Authority Function

a. Two different approaches (shown in Figure 3-1) have been agreed among the Allies for representing Release Authorities in the Allied Directory System, depending on the semantics of Release Authorities in the specifying nation. One approach is to represent the Release Authority function for an organization by having one Release Authority Role Ed. B directory entry (organizationalRole structural object class) associated with the organization. The other method is to represent each person who is a Release Authority for an organization by a Release Authority Person Ed. A directory entry (releaseAuthorityPersonA structural object class) under (i.e., named with respect to) the organization's directory entry.

b. The value "release authority" shall be the distinguished value in the commonName (naming) attribute in a Release Authority Role Ed. B directory entry.

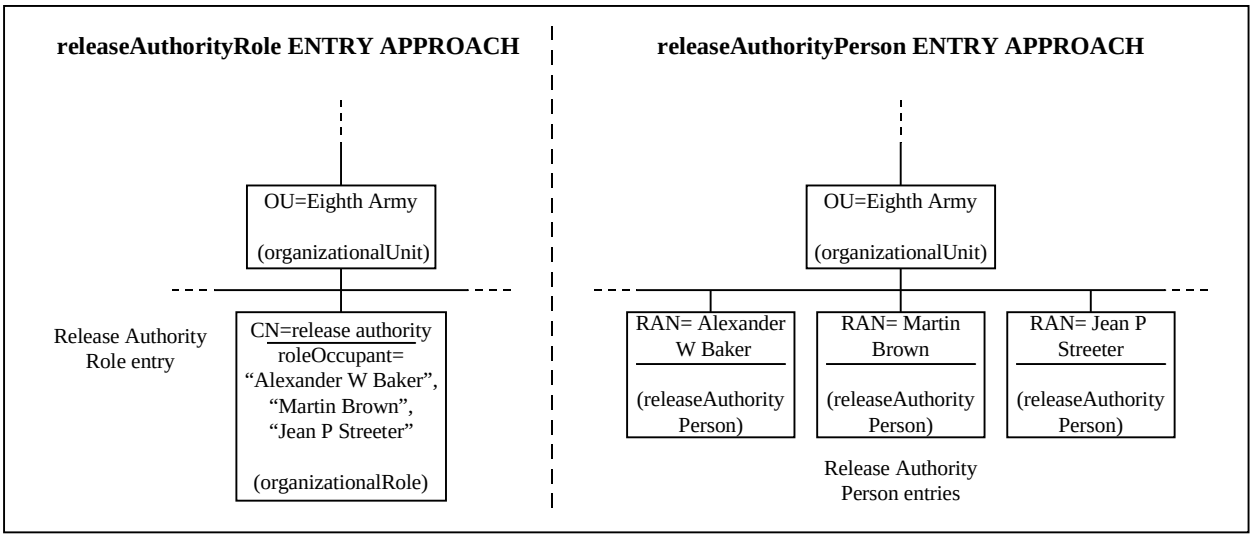

Figure 3-1
Methods of Representing Release Authorities

308. ACP 127 Users

a. In support of the ACP 127 Interworking application, two different approaches, illustrated in Figure 3-2, have been developed for representing ACP 127 users, i.e., PLAs, in the Allied Directory System, depending on the national view concerning integration of ACP 127 information with other information in the DIT. A nation may choose which method is uses in its own DIT subtree to capture PLA information; however, a national schema should support the elements of both methods in order to be able to handle PLA information that may be represented differently in other nations' DIT subtrees.

b. One method is to place PLA-related information in Organizational Unit Ed. A directory entries in the same subtrees as the information for the other applications (i.e., "share" the entries). In this case, the plaUser auxiliary object class shall be used to store the PLA and Routing Indicator (RI) in the organizational entries in the Allied Directory System. This allows the organizational subtree to be searched to find the PLA and RI information.

c. The other approach is to have separate subtrees in the DIT for PLA-related directory entries (e.g., Organizational PLA entries) and for directory entries supporting the other applications. For example, see the U.S. Top-level DIT in Annex B. Using this approach, from the ACP 127 domain, the gateway will search a PLA subtree for an associated Organizational Unit entry where an O/R address is found. From the MMHS domain to the ACP 127 domain, the Organizational Unit Ed. A entry shall have an associated PLA name which can be put in the domain-defined attribute field of the gateway address. RI information will be contained in a directory in the ACP 127 domain. Its inclusion in the X.500 Directory is a national matter.

d. Note that PLA is called Signal Address (SA) or Signal Message Address (SMA) by some nations and international or multinational organizations. Registered PLA is equivalent to SA or SMA. In this ACP, the attribute “longTitle” is defined for storing the spelled out (long form) of a PLA, SA, or SMA.

e. The purpose of the plasServed attribute is to provide the list of PLAs accessible through a gateway. It is necessary for this information to be provided by the Directory so that the X.400 address to route a message to that PLA can be created. This is of particular importance for mobile units such as ships where the gateway via which it is accessible can change. This attribute is also used to route from other types of network to ACP 127.

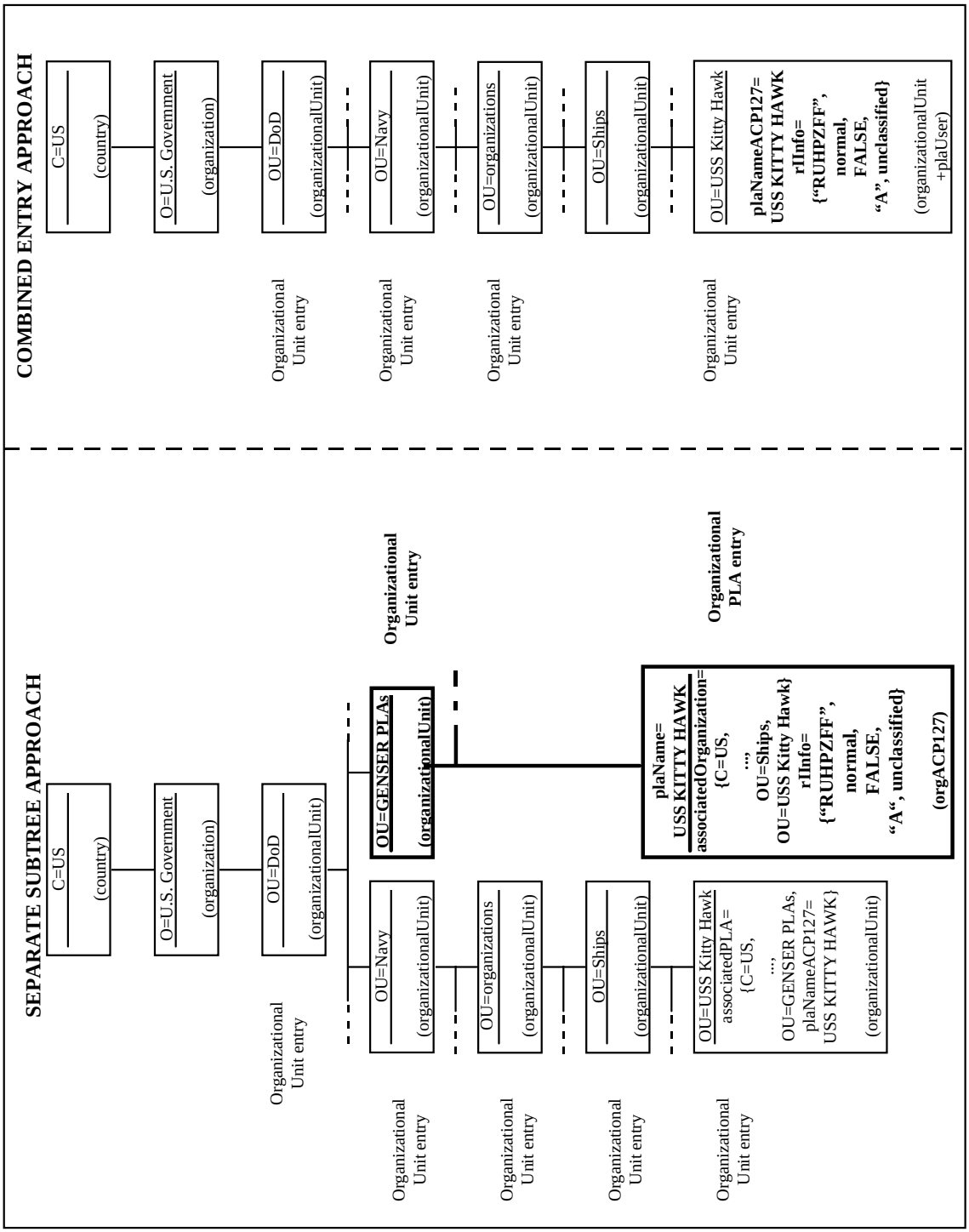

Figure 3-2
Methods of ACP 127 Interworking

309. Interconnected Telecommunication Networks

a. There is a requirement in any military voice switching network to integrate several different tactical and strategic systems. The resulting network provides support to strategic,

operational, and tactical level users. The strategic switching network provides a primary telecommunication service for strategic level users, while a tactical telecommunication network provides a primary service for operational and tactical level users. Access codes provide the means of achieving connectivity between the different types of telecommunications networks.

b. In some cases, there may be more than one route from one network to another, which may involve transiting through an intermediate network. Consequently, a number of different access codes would need to be dialed to achieve connectivity. Additionally, access codes could vary according to the locality of the network. Figure 3-3 gives an example of a number of interconnected strategic (Public Telephone Network, Network A and Local Headquarters (HQ) network) and tactical networks (B, C and D) and their associated access codes.

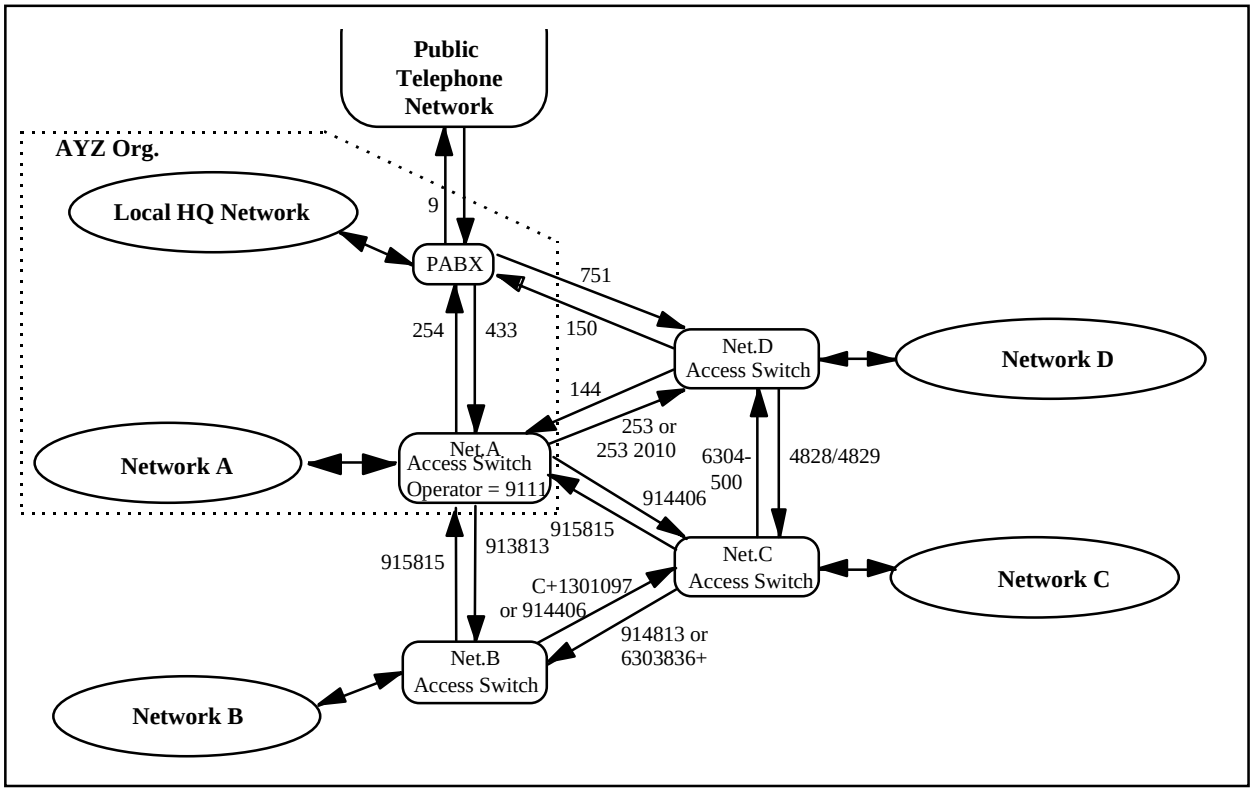

Figure 3-3
Interconnected Strategic and Tactical Networks Example

c. In order to manage the various access codes efficiently, Access Switch managers are responsible for those access codes that provide connectivity to adjacent network access switches. Hence, a set of subtrees within the DIT can be constructed that depict how one network can be reached from another; for example, Figure 3-4 depicts the access codes requirement of Network A to Network B (and vice versa) in Figure 3-3.

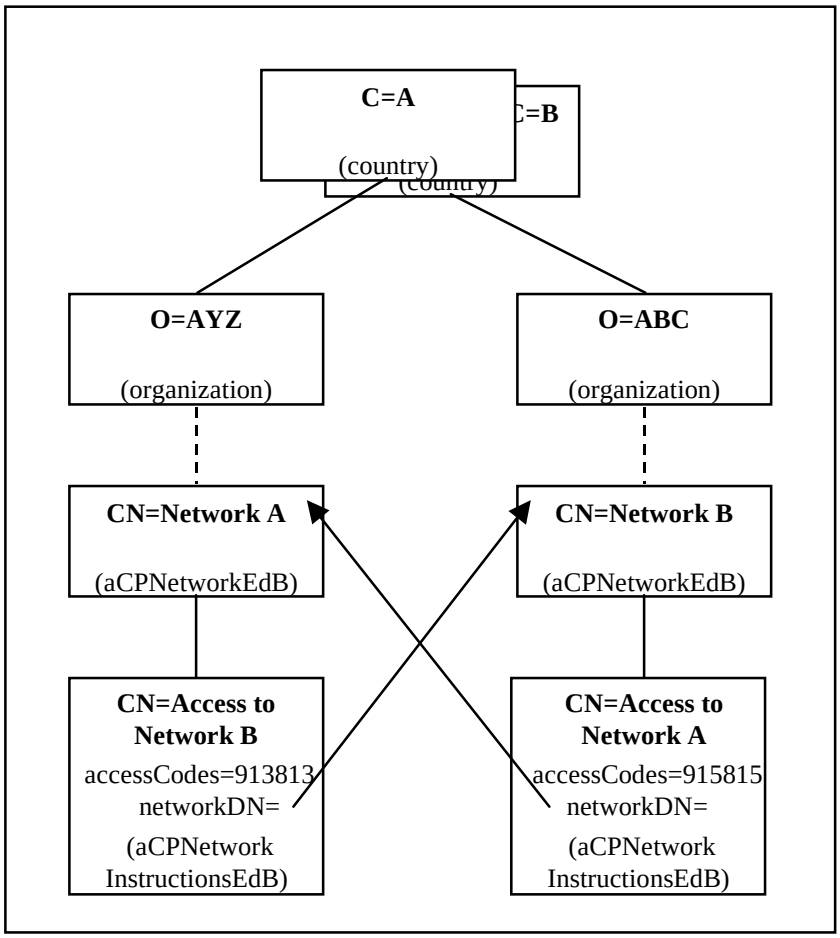

Figure 3-4
DIT Subtree Structure for Network A to Network B Access (and vice versa)

d. For completeness, Figure 3-5 depicts the total access code requirement for Figure 3-3. Although, in principle, the entries refer to “Access to” adjacent networks, the administrator may wish to include “Access to” non-adjacent networks (as denoted by a ‘*’ in Figure 3-5). In considering access between networks they can be considered as either being individual networks or can be associated with a locality, e.g., a HQ, where the user may not know on which network he resides, but knows the HQ he is in and the network or locality he wishes to access. Hence, there are four permutations for the use of access codes, either between networks, localities or both:

- network to locality
- network to network

- locality to network
- locality to locality

e. A user accessing the Allied Directory needs to be able to find the telephone number of the called party (the default being the operator), the access to the network that the called party resides upon, and any special instructions required to complete the connection. Instructions are especially important when transiting across networks that require a special instruction, like “wait for second dial tone, then dial extension”.

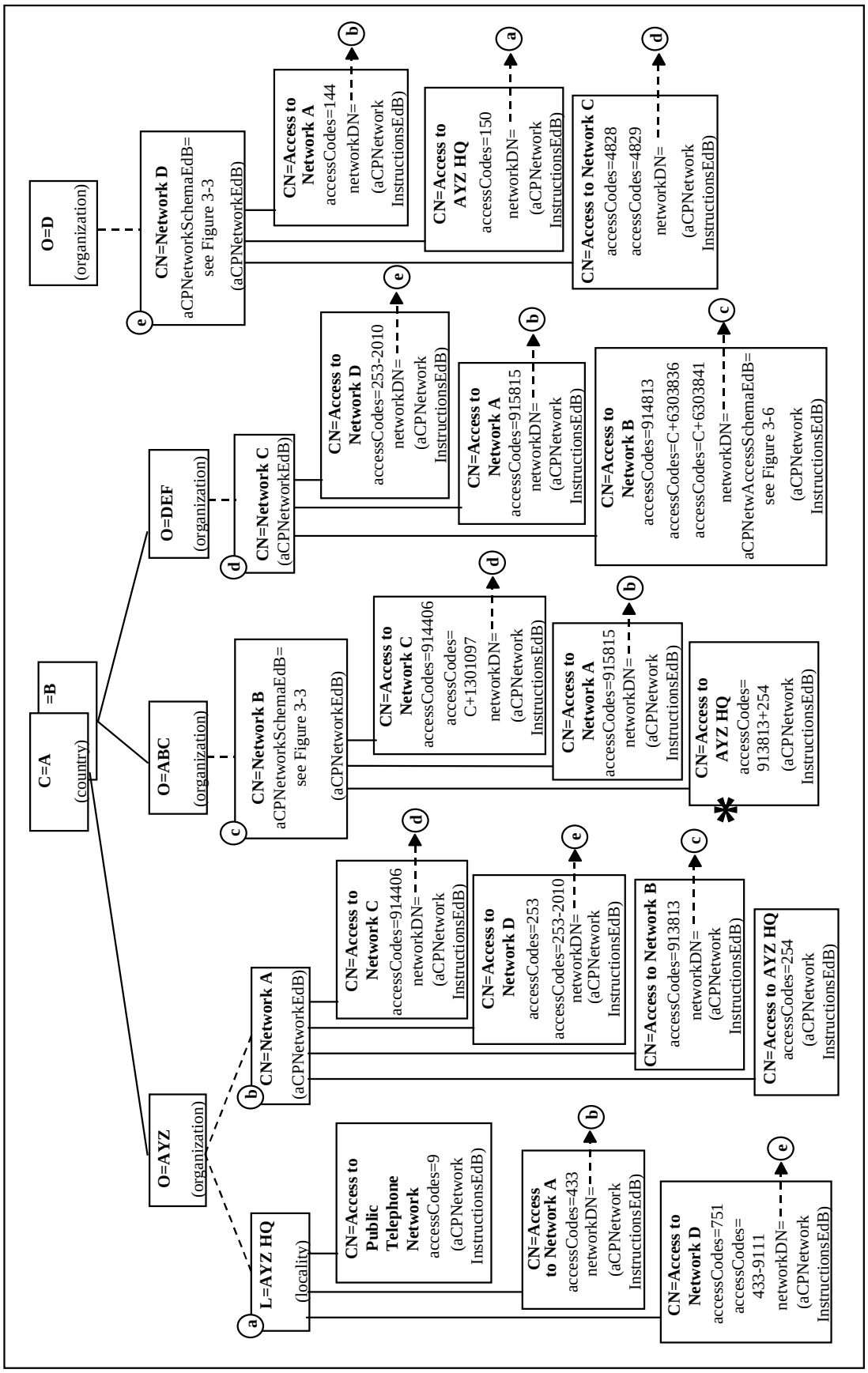

Figure 3-5
DIT Subtree Structure for Network Access Information

f. In support of providing information on telecommunications networks, two types of directory entries are defined:

- Network Ed. B
- Network Instructions Ed. B

g. Network Ed. B entries contain information about the different supported networks. They have subordinated entries that define the access instructions of how to reach other networks.

h. A Network Instructions Ed. B directory entry contains the instructions about how to reach other networks or localities from the entry above in the DIT (see Figure 3-4). When the access to another network is different from different locations, a Locality entry may have subordinated Network Instructions Ed. B directory entries.

i. Note that the new "Ed. B" entry types replace the Network and Network Instructions entry types. Also, the new entry types are based on new object classes: aCPNetworkEdB and aCPNetworkInstructionsEdB, which replace the network and networkInstructions object classes.

j. A number of attributes are used in association with the aCPNetworkEdB/aCPNetworkInstructionsEdB structural object classes as follows.

(1) In a Network Instructions Ed. B entry, the commonName attribute contains the distinguished value “Access to x”, where x is the name of the network or locality for adjacent or non-adjacent networks.

(2) The networkDN attribute value contains the full DN of a NetworkEd. B entry and may be used to reference the entry for the network from another entry. This information is particularly useful where there are too many non-adjacent networks to give instructions for all of them or the instructions for accessing a non-adjacent network change frequently. For example, during the military operation being performed by the CTF that owns the Network C, an advancing force might move across an international boundary. If connection to the Public Telephone Network of the new country is added to Network C, new alternative paths could become available that require the use of access codes appropriate to that Public Telephone Network.

(3) The aCPNetworkSchemaEdB attribute value in the Network Ed. B entry is a graphical representation of a network. It describes the structure of the network and details the rules associated with that network, such as the availability for access to a Public Telephone Network and any details of its elements of service. A possible value could be the diagram in Figure 3-3 which could be included in any or all of the Network Ed. B directory entries in Figure 3-5. Note that the aCPNetworkSchemaEdB attribute type replaces the networkSchema attribute type, in order to employ a different format for the graphics.

(4) The aCPNetwAccessSchemaEdB attribute value in the Network Instructions Ed. B entry is used to present, in a graphical/tabular form, the different connection options between the pair of network interconnections. An example of a tabular description of the interconnection of two networks is given in Figure 3-6. Another use for the aCPNetwAccessSchemaEdB attribute is to take advantage of the Network Instructions Ed. B entry being specific to one other network in order to make it easier for the user to locate the information necessary for a particular connection. Note that the aCPNetwAccessSchemaEdB attribute type replaces the accessSchema attribute type, in order to employ a different format for the graphics.

(5) The accessCodes attribute value is used to hold the actual codes used to reach one network from another. These values may also be shown in the accessSchema attribute. It also contains additional instructions, such as, when it is necessary to wait for an operator to connect, then followed by dialing the desired extension number.

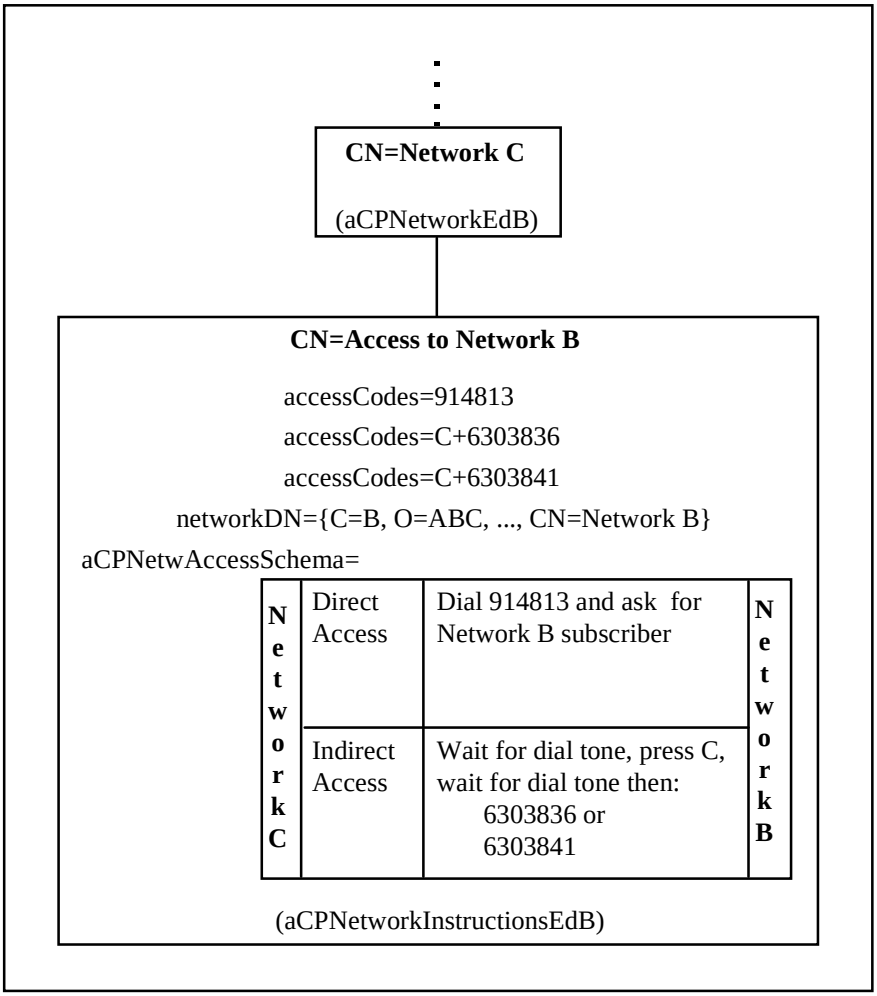

Figure 3-6
Example of an aCPNetwAccessSchemaEdB for Network B

310. Use of the seeAlso Attribute

The correct use of the seeAlso attribute can benefit Allied Directory System users. Conversely poor use of the attribute can have an adverse effect on performance of the Allied Directory System and create frustration for users and additional burden for directory administrators. It is the responsibility of the directory administrator to ensure that the seeAlso attribute values are valid and do not point to non-existent directory entries. The procedural recommendations for the use of the seeAlso attribute in each of the relevant directory entry types are given below. In all cases, the seeAlso attribute is optional.

a. Application Entity Ed. A

The seeAlso attribute for the Application Entity may be used to point to other Application Entity Ed. A directory entries. Specific types of application entity covered separately include DSA, MLA, MHS UA, etc.

b. Device Ed. A

The seeAlso attribute for the Device may be used to point to other Device Ed. A directory entries. Examples would be pointers to printers with similar capabilities.

c. DSA Ed. A

The seeAlso attribute for the DSA may be used to point to other DSA Ed. A directory entries. For example, it may point to a DSA providing back-up to this DSA.

d. MHS Distribution List

The seeAlso attribute for the MHS Distribution List may be used to point to other MHS Distribution List directory entries. No specific use has been identified at this time.

e. MHS Message Store Ed. A

The seeAlso attribute for the MHS Message Store Ed. A may be used to point to other MHS Message Store Ed. A directory entries. No specific use has been identified at this time.

f. MHS Message Transfer Agent Ed. A

The seeAlso attribute for the MHS Message Transfer Agent Ed. A may be used to point to other MHS Message Transfer Agent Ed. A directory entries. The other directory entries could be for MTAs with the same type of function in a domain, such as, backbone MTAs that serve the same geographic area.

g. MHS User Agent

The seeAlso attribute for the MHS User Agent may be used to point to other MHS User Agent directory entries. No specific use has been identified at this time.

h. Organization Ed. B

The seeAlso attribute for the Organization Ed. B may be used to point to other Organization Ed. B directory entries. Whether this would be useful is questionable because of the high level of organizations in the DIT, for example, NATO.

i. Organizational Person Ed. B

The seeAlso attribute for the Organizational Person Ed. B may be used to point to other Organizational Person Ed. B directory entries. These other Organizational Person Ed. B directory entries shall be from the same organization or organizational unit, physically close, or have similar functional duties to the source entry person. A possible use is a pointer to another identity for an organizational person, such as, in a combined domain. It could also be used to point to the Organizational Role Ed. B directory entries which designate the organizational person as a role occupant.

j. Organizational Role Ed. B

The seeAlso attribute for the Organizational Role Ed. B may be used to point to other Organizational Role Ed. B directory entries. These other Organizational Role Ed. B directory entries shall be from the same organization or organizational unit, physically close, or have similar functional duties to the source entry.

k. Organizational Unit Ed. B

The seeAlso attribute for the Organizational Unit Ed. B may be used to point to other Organizational Unit Ed. B directory entries. These other Organizational Unit Ed. B directory entries shall be from the same organization, physically close to, or have similar functional duties to that of the source entry. A possible use is a pointer to a portion of an organizational unit which has been deployed and is part of a combined domain.

l. Address List Ed. A

The seeAlso attribute for the Address List Ed. A may be used to point to other Address List Ed. A directory entries. No specific use has been identified at this time.

m. Application Process

The seeAlso attribute for the Application Process may be used to point to Application Entity Ed. A and other Application Process directory entries. No specific use has been identified at this time.

n. Group of Names

The seeAlso attribute for the Group of Names may be used to point to other Group of Names directory entries. No specific use has been identified at this time.

o. Locality

The seeAlso attribute for the Locality may be used to point to other Locality directory entries. No specific use has been identified at this time.

p. Messaging Gateway Ed. A

The seeAlso attribute for the Messaging Gateway Ed. A may be used to point to other Messaging Gateway Ed. A directory entries. These other Messaging Gateway Ed. A directory entries shall have the same capability, e.g., translation between ACP 127 and ACP 123 messaging networks, and belong to the same domain.

q. MLA Ed. A

The seeAlso attribute for the MLA Ed. A may be used to point to other MLA Ed. A directory entries. The attribute could point to another MLA responsible for the same mail lists.

r. Release Authority Role Ed. B

The seeAlso attribute for the Release Authority Role may be used to point to other Release Authority Role Ed. B and Organizational Role Ed. B directory entries. No specific use has been identified at this time.

SECTION II

ENTRY AND ATTRIBUTE POPULATION AND USAGE

311. Population Requirements and Guidelines for Various Types of Communications

a. This section is intended for administrators who are planning for or are populating the directory entries in the Allied Directory System. Population refers to the directory entries and attributes for which values should be made available in the Allied Directory to support given user applications. The minimal subset of the Common Content that needs to be populated for various communication applications is stated in this section. (See Annex B for specification of the Common Content.) The types of applications for which population requirements are stated are:

- e-mail communication (non-X.400)
- Secure Multi-purpose Internet Mail Extension (S/MIME)
- commercial MHS communication

- MMHS communication
- communication between MMHS users and ACP 127 users
- traditional communications (e.g., telephone, facsimile, and postal mail)

b. Table 3-1 indicates the directory entries required. Table 3-2 indicates the required auxiliary object classes for directory entries. Tables 3-3 through 3-21 indicate the associated attributes for which values are necessary to support each application.

c. For e-mail communication (non-X.400), the directory entries and attributes shall contain the common name and e-mail (RFC 822) address.

d. For S/MIME communication, the directory entries and attributes shall contain the common name, e-mail (RFC 822) address, and user certificate.

e. For commercial Message Handling System (i.e., civilian X.400) communication, the directory entries and attributes shall contain the information necessary for performing the core functions of a messaging system. These functions include, but are not restricted to: addressing, routing, expanding address lists, and directory access.

f. For MMHS and e-mail services with confidentiality and digital signature features, the directory entries and attributes shall contain the information necessary for performing the core functions of a secure messaging system. These functions include: addressing, routing, securing a message, translating from one type of messaging protocol into another, expanding address lists, and directory access.

g. For interworking between the ACP 127 and MMHS systems, the directory entries and attributes shall contain the information necessary to identify and characterize ACP 127 users and to utilize the gateway(s) between the two systems.

h. In order to support traditional communication services, such as, telephone, facsimile, and postal mail, the directory entries and their associated attributes shall contain the information necessary for human users to look up someone else's information by providing a common name of an organizational person or organizational role, or the organizational unit name of an organization. The directory serves as a repository of this information, and after the user gets the information from the directory, the rest of the communication takes place using the traditional communications network.

i. Table 3-1 indicates, for each application, the directory entries that are necessary for Allied communication whether specified by the standards or in the Abstract Syntax Notation One (ASN.1) definitions in this ACP. If the directory entry is required, then it is indicated by a "•" to highlight that the Allied Directory shall contain directory entries of that type.

Table 3-1
Population of Directory Entries for Applications

Entry Type	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. Address List Ed. A				•	•	
2. Application Entity Ed. A	•	•	•	•	•	•
3. Certification Authority Ed. B		•		•		
4. CRL Distribution Point		•		•		
5. DSA Ed. A	•	•	•	•	•	•
6. Group of Names		•		•		•
7. Messaging Gateway Ed. A	•	•	•[2]	•[2]	•	
8. MHS Message Store Ed. A			•[2]	•[2]		
9. MHS Message Transfer Agent Ed. A			•[2]	•[2]		
10. MLA Ed. A				•[2]		
11. Organizational Person Ed. B	•	•	•	•		•
12. Organizational PLA					•[1]	
13. Organizational Role Ed. B	•	•	•	•		•
14. Organizational Unit Ed. B		•	•	•	•	•
15. PLA Collective					•	
16. Release Authority Person Ed. A				•[3]		
17. Release Authority Role Ed. B				•[3]		
18. Task Force PLA					•	
19. Tenant PLA					•	

[1] The requirement shown applies only when the "separate subtree" method is employed, as described in paragraph 308.

[2] These entries must be populated where the messaging system is built to make use of them.

[3] One of Release Authority Person Ed. A or Release Authority Role Ed. B needs to be populated.

j. In addition, entries for Country, Organization, Organizational Unit, and Locality may need to be populated in order to provide structure for a nation's DIT.

k. Table 3-2 indicates the auxiliary object classes, which are optional in the Common Content (i.e., a class that is added to an entry type using a content rule; see Annex B), that some applications require for a certain entry type. If the auxiliary object class is required by an

application, then it is indicated by a "•" to highlight that the auxiliary object class's object identifier shall be included in the object class attribute in the directory entry.

Table 3-2
Auxiliary Object Classes Required in Directory Entries for Applications

Entry Type and Auxiliary Object Classes	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. Address List Ed. A						
distributionCodesHandled						
mhs-user				•		
plaUser					•[1]	
securePkiUser				•		
ukms						
2. Certification Authority Ed. B[2]						
pkiCA		•		•		
3. DSA Ed. A						
securePkiUser	•	•	•	•	•	•
4. Messaging Gateway Ed. A						
securePkiUser		•		•		
ukms						
5. MHS Message Store Ed. A						
securePkiUser				•		
6. MHS Message Transfer Agent Ed. A						
securePkiUser				•		
7. Organizational Person Ed. B						
distributionCodesHandled						
mhs-user			•	•		
otherContactInformation						•
securePkiUser		•[3]		•		
ukms						

Table 3-2
Auxiliary Object Classes Required in Directory Entries for Applications

Entry Type and Auxiliary Object Classes	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
8. Organizational Role Ed. B						
pkiCA						
distributionCodesHandled						
mhs-user			•	•		
otherContactInformation						•
securePkiUser		•[3]		•		
ukms						
9. Organizational Unit Ed. B						
distributionCodesHandled						
mhs-user			•	•		
otherContactInformation						•
plaUser					•[1]	
securePkiUser		•[3]		•		
ukms						

[1] The requirement shown applies only when the "combined entry" method is employed, as described in paragraph 308.
[2] Requirements for auxiliary object classes, other than pkiCA, are the same as for the entry type (Organization Ed. B, Organizational Role Ed. B, Organizational Unit Ed. B, or Application Entity Ed. A) as the nation is using for representing CAs.
[3] S/MIME requires population of pkiUser which is a superclass of securePkiUser.

l. Tables 3-3 through 3-21 indicate, for each application, the directory entry's attributes that are necessary for Allied communication including those mandated by the standards or in the ASN.1 definitions in this ACP. If the attribute is required for any of these reasons, then it is indicated by a "•" to highlight that the attribute value shall be "populated" (i.e., the attribute has a value). Attributes listed under the directory entries are a combination of the attributes included in the entry type's structural object class (including those attributes included in the base object class and those attributes inherited from superclasses) and the auxiliary object classes and additional attributes added to that entry. All attributes that require values shall include a non-null value. Exceptions are:

- attribute values for which a value does not exist
- attributes required by the standards that are not used by the ACP 133
- attributes where population is prohibited by the user's security policy

m. Specific exceptions to populating the attributes are highlighted in the following paragraphs.

Table 3-3
Population of Address List Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName				•	•	
2. copyMember[1]				•	•	
3. description				•	•	
4. mhs-dl-submit-permissions				•	•	
5. mhs-or-addresses				•	•	
6. mhs-or-addresses-with-capabilities[2]				•	•	
7. owner				•	•	
8. member[1]				•	•	
9. userCertificate				•	•	

[1] An Address List entry shall have values in the member attribute or copyMember attribute or both.

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-4
Population of Application Entity Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName	•	•	•	•	•	•
2. presentationAddress	•	•	•	•	•	•

n. Table 3-5 includes information used to send messages to a CA represented by a Certification Authority Ed. B entry. This table indicates for each application, the population requirements for the attributes in the pkiCA auxiliary object class, in addition to the requirements for the Organization Ed. B, Organizational Role Ed. B, Organizational Unit Ed. B, or Application Entity Ed. A entry type of which the Certification Authority Ed. B directory entry type is a special case.

Table 3-5
Population of Certification Authority Ed. B[1]

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. authorityRevocationList		•		•		
2. cACertificate		•		•		
3. certificateRevocationList		•		•[2]		
4. crossCertificatePair[3]		•		•		

[1] The attributes in this table are in addition to whatever attributes may also be populated in the entry, as a result of the structural and other object classes to which the entry also belongs.

[2] Alternatively, certificateRevocationList may be populated in a CRL Distribution Point entry.

[3] The forward certificate within the cross certificate pair shall be present; the reverse certificate should be present, if it is available.

Table 3-6
Population of CRL Distribution Point

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. authorityRevocationList		•		•		
2. certificateRevocationList		•		•		
3. commonName		•		•		

Table 3-7
Population of DSA Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName	•	•	•	•	•	•
2. presentationAddress	•	•	•	•	•	•
3. supportedAlgorithms	•	•	•	•	•	•
4. userCertificate	•	•	•	•	•	•

Table 3-8
Population of Group of Names

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName		•		•		
2. member		•		•		

o. In Table 3-9, each of the columns represents a level of service that can be implemented in a gateway being used for interworking between MMHS domains and other messaging domains (i.e., e-mail, commercial MHS, MMHS, and ACP 127).

Table 3-9
Population of Messaging Gateway Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName	•	•	•	•	•	
2. mhs-or-addresses			•	•	•	
3. mhs-or-addresses-with-capabilities[1]			•	•	•	
4. plasServed					•	
5. presentationAddress	•	•	•	•	•	
6. rfc822Mailbox	•	•				
7. supportedAlgorithms		•		•	•	
8. userCertificate		•		•	•	

[1] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-10
Population of MHS Message Store Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName			•	•		
2. presentationAddress			•	•		

Table 3-11
Population of MHS Message Transfer Agent Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName			•	•		
2. presentationAddress			•	•		
3. supportedAlgorithms				•		
4. userCertificate				•		

Table 3-12
Population of MLA Ed. A

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. commonName				•		
2. presentationAddress				•		
3. supportedAlgorithms				•		
4. userCertificate				•		

Table 3-13
Population of Organizational Person Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. aCPMobileTelephoneNumber						•[1]
2. commonName	•	•	•	•		•
3. dnQualifier	•[1]	•[1]	•[1]	•[1]		•[1]
4. facsimileTelephoneNumber						•[1]

Table 3-13
Population of Organizational Person Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
5. mhs-or-addresses			•	•		
6. mhs-or-addresses-with-capabilities[2]			•	•		
7. militaryFacsimileNumber						•[1]
8. militaryTelephoneNumber						•[1]
9. organizationalUnitName	•	•	•	•		•
10. postalAddress						•
11. proprietaryMailboxes	•[1]					
12. rfc822Mailbox	•	•				
13. secureFacsimileNumber						•[1]
14. secureTelephoneNumber						•[1]
15. supportedAlgorithms		•		•		
16. telephoneNumber						•[1]
17. userCertificate		•		•		

[1] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number then an attribute value shall not be included in the attribute).

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-14
Population of Organizational PLA

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking [1]	Traditional Communications
1. associatedOrganization					•	
2. countryName					•[2]	

Table 3-14
Population of Organizational PLA

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
3. effectiveDate					•[2]	
4. localityName					•[2]	
5. longTitle					•[2]	
6. plaNameACP127					•	
7. remarks					•[2]	
8. rIInfo					•[3]	

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

[2] These attributes are used when the directory is used to store ACP 117 information (i.e., publish ACP 117).

[3] This attribute is populated when the directory implementation supports use of RI information.

Table 3-15
Population of Organizational Role Ed. B

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. aCPMobileTelephoneNumber						•[1]
2. commonName	•	•	•	•		•
3. facsimileTelephoneNumber						•[1]
4. mhs-or-addresses			•	•		
5. mhs-or-addresses-with-capabilities[2]			•	•		
6. militaryFacsimileNumber						•[1]
7. militaryTelephoneNumber						•[1]
8. roleOccupant	•	•	•	•		•
9. postalAddress						•

Table 3-15
Population of Organizational Role Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
10. proprietaryMailboxes	•[1]					
11. rfc822Mailbox	•	•				
12. secureFacsimileNumber						•[1]
13. secureTelephoneNumber						•[1]
14. supportedAlgorithms		•		•		
15. telephoneNumber						•[1]
16. userCertificate		•		•		

[1] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number then an attribute value shall not be included in the attribute).

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-16
Population of Organizational Unit Ed. B

Attribute	E-MAIL	S/MIME	Commercial MHS	MMHS	ACP 127 Interworking	Traditional Communications
1. aCPMobileTelephoneNumber						•[2]
2. associatedPLA					•[1]	
3. facsimileTelephoneNumber						•[2]
4. mhs-or-addresses			•	•		
5. mhs-or-addresses-with-capabilities[3]			•	•		
6. militaryFacsimileNumber						•[2]
7. militaryTelephoneNumber						•[2]
8. organizationalUnitName		•	•	•		•

Table 3-16
Population of Organizational Unit Ed. B

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
9. plaNameACP127					•[4]	
10. postalAddress						•
11. rfc822Mailbox		•				
12. secureFacsimileNumber						•[2]
13. secureTelephoneNumber						•[2]
14. supportedAlgorithms		•		•		
15. telephoneNumber						•[2]
16. userCertificate		•		•		

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

[2] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number then an attribute value shall not be included in the attribute).

[3] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

[4] The requirements shown for this application apply when the "combined entry" method is employed, as described in paragraph 308.

p. A PLA Collective directory entry shall be used when a pointer is necessary to check on the validity of a PLA, e.g., for Type Organization Collectives.

Table 3-17
Population of PLA Collective

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
1. associatedAL					•	
2. plaNameACP127					•	

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

Table 3-18
Population of Release Authority Person Ed. A

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
1. releaseAuthorityName				•		
2. supportedAlgorithms				•		
3. userCertificate				•		

q. Table 3-19 includes information used to send messages to a Release Authority, which is represented by a Release Authority Role Ed. B entry.

Table 3-19
Population of Release Authority Role Ed. B

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. commonName	•		•	•		•
2. facsimileTelephoneNumber						•[1]
3. mhs-or-addresses			•	•		
4. mhs-or-addresses-with-capabilities[2]			•	•		
5. militaryFacsimileNumber						•[1]
6. militaryTelephoneNumber						•[1]
7. mobileTelephoneNumber						•[1]
8. roleOccupant	•		•	•		•
9. postalAddress						•
10. proprietaryMailboxes	•[1]					
11. rfc822Mailbox	•					
12. secureFacsimileNumber						•[1]
13. secureTelephoneNumber						•[1]
14. supportedAlgorithms				•		
15. telephoneNumber						•[1]
16. userCertificate				•		

[1] Population of the attribute is dependent upon the user having a value for the attribute (e.g., if the user does not have a mobile telephone number, then an attribute value shall not be included in the attribute).

[2] Applies only if there are multiple O/R addresses in the entry or if there is a need to associate a security label with an O/R address.

Table 3-20
Population of Task Force PLA

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working [1]	Tradi-tional Com-munica-tions
1. associatedAL					•	
2. plaNameACP127					•	

[1] The requirements shown for this application apply when the "separate subtree" method is employed, as described in paragraph 308.

Table 3-21
Population of Tenant PLA

Attribute	E-MAIL	S/MIME	Com-mercial MHS	MMHS	ACP 127 Inter-working	Tradi-tional Com-munica-tions
1. hostOrgACP127					•	
2. plaNameACP127					•	

SECTION III

REGISTRATION

312. Registration Requirements

The following objects need to be registered to ensure that they are unique with a global context of the Allied Directory:

- technical object identifiers
- directory DNs
- other information stored in the directory, e.g., addresses

313. Technical Object Identifier

a. Object identifiers provide a unique reference to the definition of technical objects. This includes technical objects which are specific to the directory such as object class and attribute definitions, as well as technical objects which have wider relevance such as certificate policy identifiers. Other applications such as Open Systems Interconnection (OSI) management and messaging also make use of object identifiers to reference technical definitions.

b. Object identifiers for standard technical definitions are allocated in the standard where they are defined (e.g., X.500 allocates object identifiers for directory object classes and attributes defined in that standard).

c. Object identifiers for new schema definitions for object classes, attributes, name forms, etc., for the Allied Directory are defined in this ACP (see Annex B) under the object identifier:

{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) ds(2) }

d. National or other new schema definitions outside the scope of this ACP are allocated object identifiers under the appropriate national or international object identifier registration scheme.

314. Distinguished Name

a. A DN is a sequence of naming attributes which uniquely identify an object which may be represented by an entry in the directory. Objects that may be identified using a distinguished name include organizational units, people, roles, address lists, devices, application entities, and release authorities. A distinguished name is used as the primary "key" to locate an entry in the Allied Directory. In addition, distinguished names are used to identify the subject of an X.509 public key certificate.

b. The naming attributes which form a DN are organized in a hierarchy reflecting the DIT with a name lower in the tree identified relative to its parent entry by adding RDN attributes to the parent's DN.

c. Before an entry is created for an object in the directory (or a certificate created for that object) it must be allocated a DN which is unique. The allocation of a distinguished name in the Allied Directory is the responsibility of the Registration Authority for the Service, agency, or command to which the named object belongs. A registration authority may delegate responsibility of directory distinguished name registration for subtrees within its domain to Sub-Registration Authorities. A registration authority (or sub-registration authority) may also take on responsibility for registration of other identifiers including technical object identifiers and addresses (see below).

d. The DNs used at the top levels of Allied directory domains are given in Annex B.

e. The registered DNs relevant to the Allied Directory may be disseminated through the directory.

315. General Registration Requirements

a. The directory can be used to store addressing and other related information. As with DNs these addresses need to be unique within the global context and hence must be allocated under a registration scheme. Examples of information requiring registration are X.400 MHS Addresses (including Private Management Domain (PRMD) identifiers), OSI network addresses, and Internet Protocol addresses.

b. The specific registration requirements for the registration of information such as addresses is dependent on the type of communication or application service to which the information applies, and is hence outside the scope of this ACP. However, objects which are allocated DNs commonly also require addresses (e.g., X.400 addresses) and, hence, the various registration functions should be coordinated using coherent registration procedures.

c. Common Allied registration guidelines are recommended. This should cover procedures for coordination, dissemination, and ratification of registration information, such as:

- technical objects identifiers defined for Allied use
- DNs used in the Allied context
- X.400 addresses

SECTION IV

SHADOWING

316. Shadowing Policy

a. A Shadowing Agreement Checklist is initiated by the administrator of the supplier DSA, who administers the information requiring shadowing. The Shadowing Agreement Checklist is filled out and provided to the consumer DSA administrator for completion and agreement. The Shadowing Agreement is reviewed and approved by the Directory Services Manager. The agreement shall state the protection provided to shadowed information. Also, when agreement involves secondary shadowing, the Shadowing Agreement Checklist is reviewed and approved by the DSA Administrator of the Master DSA. Annex E gives an example of a Shadowing Agreement Checklist, including the standard X.500 shadowing agreement parameters.

b. Directory information that is provided to the Allied Directory System from national directories may be shadowed, and individual entries within this information may be incomplete. Thus, users may not find what they are looking for and require access to the master or a complete

replicated entry. In a directory system unconstrained by access controls, users would be able to satisfy the request by chaining from the Border DSA into the national directory. However, this situation may not be permitted. In order to satisfy one nation's directory queries of another nation's Border DSA, consideration should be given to the way in which replicated data is marked. The options are that the data may be marked as a master or copy. If it is a copy, it may be marked as incomplete. If it is marked as incomplete, it implies that chaining is permitted into the directory that contains the complete entry. This may be a national DSA or another Border DSA. How data is marked should be specified within the allied Service Level Agreements (SLAs).

SECTION V

DIRECTORY SYSTEM PERFORMANCE

317. General

The Allied and the supporting national directories, which combine to form an overall directory service capability for the allied forces, must have realistic performance characteristics. Performance can be seen in a number of ways namely: ease of use, robustness, timeliness of service restoration, and speed of access response.

a. Ease of Use

Ease of use is a factor of the system design and the tools presented to the directory user such as click and point, icons, windows, scripts, status messages, etc. This aspect of the system is beyond the scope of this document but will be subject to national system Concepts of Operations (CONOPS), policies, and procurement procedures.

b. Robustness

Robustness deals with product and system reliability and integrity. Again, these will have to be specified in terms of Integrated Logistics Support (ILS) and Life-Cycle Costing (LCC) needs and Mean Time Between Failure (MTBF)/Mean Time To Repair (MTTR) type specifications. This is also beyond the scope of this document.

c. Availability

The goal is to provide 24 by 7 availability of the Allied Directory Service.

d. Service restoration

Service Restoration deals with the recovery time for a single DSA to attain an operational state after switch on or switching the DUAs (and other attached DSAs) to an alternate DSA. This should not exceed five minutes if the DSA is in a strategic environment. In a tactical environment, it should be less than one minute.

e. Speed of Response

(1) For defining the speed of response requirements, the directory system can be seen to provide two types of access characteristics. These are:

- the human access requirements, which deal with organizational information retrieval (such as postal and telecommunications information) via a man-machine interface

- specific system functions (such as MTAs and UAs), which need to resolve for example, names to addresses for message routing. This interface is considered to be a machine-to-machine interface.

(2) Both of the above have performance requirements. However, how these are characterized and presented can be quite different. Underlying the performance of such a large scale system is naturally the individual DSA performance and the links used between them to other DSAs and the accessing DUAs. It is outside the scope of this document to provide specifics of these, except that some general guidelines are provided to assess the capability of a DSA platform and determine its accessibility and performance in a distributed environment.

318. Human Interfaces

a. In terms of specifics, the human interface and its response requirements set the directory performance requirements and thus impose the directory system design.

b. The directory user interface performance requirement is as follows:

(1) All interrogation accesses satisfied in the home DSA shall be performed within three seconds for a ten-kilobyte retrieval.

(2) 95 percent of the intra-domain interrogation accesses shall be satisfied within five seconds for a ten-kilobyte retrieval. Worst case shall not exceed ten seconds.

(3) 90 percent of the inter-domain interrogation accesses shall be satisfied within 15 seconds for a ten-kilobyte retrieval. Worst case shall not exceed 20 seconds.

(4) An update operation to a single entry shall be performed within five seconds.

319. First-level DSAs

Performance requirements for access to first-level DSAs (FLDSA) are derived from the requirement for passing messages according to their precedence/priority in specified times as described in ACP 123 and shown in Table 3-21. All accesses to directories which serve the Message Transfer System (MTS) and the transfer of a message must not jeopardize the messaging throughput requirements. A few guidelines can be given.

a. For any Allied scenario, each FLDSA in the system should route DAP or DSP requests to its adjacent DSA in less than 500 milliseconds.

b. For any Allied scenario, each FLDSA in the system should be able to replicate into its country and direct organizational level entries (to a maximum of 12 entries, e.g., eight Country plus four organization entries) in less than two seconds.

c. For any Allied scenario, each FLDSA in the system which detects failure in protocol operations (DAP, DSP, DISP), should signal its attached ADUA or management center within one second.

d. For any Allied scenario, where any FLDSA fails and goes off line, a standby should be operational within 30 seconds and any reconfiguring of replication agreements achieved in one minute.

e. Each FLDSA in the system should be provided with sufficient processing and storage resource to assemble fragmented Search and List results of 200 entries in less than one second.

f. Each FLDSA in the system should be synchronized to a responsible time source with a maximum deviation of five seconds from other FLDSAs.

320. System Function Access

a. Military Messaging

(1) This type of access serves the allied messaging system's processing entities. These entities are typically messaging UAs, MTAs, MLAs, CAs, Profiling User Agents and Gateways (tactical, security, etc.) that incorporate DUA functions.

(2) Most of the above will access their associated directories for very specific needs such as list expansion, name to address translation or user submission/delivery capability testing. In terms of specifying performance for the combined messaging and directory system, the overall capability is to pass messages according to their precedence/priority in specified times. This is specified in ACP 123. For instance, a Flash (Urgent) message must traverse the allied MTS within three minutes. Therefore, all accesses to the directories which serve the MTS and the transfer of this message must not jeopardize the messaging throughput requirement.

(3) How many accesses to directories will occur along any specific MTS transfer path cannot be accurately determined without hard configuration information, but it is considered that nominally, there could be five directory accesses with a worst case of ten. The total time for these accesses shall be less than 20 percent of the overall message transit time requirement (for Flash messages).

(4) Table 3-22 reflects this for the various message precedence levels. Naturally, only generalized access speeds are provided. For example, for the worst cases (Non-Urgent <= eight hours), it is unlikely for a DSA to take the full 60 seconds if it is locally accessed by the

respective MTA and the information required is contained in it. However, the requirement for servicing Override and Flash messages shall be strictly observed.

Table 3-22
MHS-derived Directory System User Speed of Query Requirements

Military Precedence	MTS Grade of Delivery/Directory Priority	Originator-to-Recipient Time of Delivery	MTS Time of Delivery	Directory Speed of Query Requirement*
OVERRIDE	URGENT/high	3 min.	≤3 min.	2.5 sec.
FLASH		10 min.		
IMMEDIATE	NORMAL/ medium	20 min.	≤20 min.	7.5 sec.
PRIORITY		45 min.		
ROUTINE	NON-URGENT/ low	≤ 8 hours or start of next business day	≤ 8 hours or start of next business day	30 sec.
DEFERRED				

* These values assume that the DUA has already performed a Bind operation with the DSA. If the DUA is not bound, the combined bind and query shall take no more than twice as long as indicated here.

(5) It should be noted that there is no formal way in which an MTA, because of message priority/precedence, will set or test the time a directory query takes. This is a product design and implementation issue. The Allies should seek implementations where the message priority is reflected in the directory access priority in service controls between the MTA and DSA which service that message.

(6) It should also be noted that there is no formal way in which a messaging user can, during the construction of a message, request that the DSA perform directory accesses at a priority in line with the message precedence proposed, unless the precedence field is provided before related Military Messaging User Agent (MMUA) directory accesses are performed and the implementation ties the access priority to the message precedence.

(7) Thus, directory performance levels can be realistically requested only for dealing with message transfer through the MTS from the point of submission.

b. Other Applications

The Allied Directory System will be accessed for other purposes than supporting the messaging function. Examples of functions for which the performance criteria for directory access may be different from the messaging support criteria are:

- authenticating management entities
- distributing certificate revocation lists (CRLs)

321. Performance Characteristics

The following text provides some generalized notes that should be applied in the procurement, design, and operation of the directory systems for both the national systems and the shared/combined systems.

a. DUA Selection of Priority

In the human interface, there may be an option for selecting directory access priority. Such a feature must be used responsibly, considering DSA capacity and the relative urgency of the request. The default for priority should be set to normal. It is recommended that Urgent Priority directory accesses be reserved for tactical operations.

b. DSA Priority Processing

DSAs should be capable of servicing the priority field. However, this will depend on the queuing, processing architecture, and DIT storage mechanisms that a DSA uses. Suffice it to say that the operations in the input queues of a DSA must be serviced according to priority.

c. DAP Service Parameters

The Size Limit and Time Limit Service Control parameters should be defaulted to catch/inhibit any unexpectedly large (gigabyte) responses or dead DSAs in the chain. For example, Size Limit is defaulted to the number of objects that can be contained in 250 kilobytes.

d. DSA Performance Reporting

The DSAs shall provide performance reports which demonstrate characteristics of population, speed of access, speed of basic and filtered searches, and DIT modification/replication actions.

e. DSA Association Limits

All DSAs shall support at least 100 simultaneous associations.

f. DSA Bind Time Limits

It shall take less than ten seconds for a DSA to perform a Bind or Unbind with strong authentication with a DUA or other DSA.

g. Bogus Searches

When a search for a bogus entry is instigated (e.g., find bogus entry), the response shall be returned in less than 30 seconds, preferably ten.

h. Access Control Processing

When access controls are applied to Reads, Lists, and Searches, etc., to restrict access to identified users, they shall not increase access time by more than ten percent of the time for unrestricted access.

i. Chained Operations

When a Search is chained by a DSA (using DSP), it is a DSA performance requirement that Search requests to the other DSAs shall be initiated within ten seconds of the initial DSA access.

j. Performance Optimization Tools

It is possible that, as the allied system evolves, utilities will be developed that do scripted actions on the directory system. To assist in performance optimization of the Allied Directory System, some form of service logging and tuning tools must be used.

k. Alias/List Utilities For DIT Integrity

To assist in DIT management, alias integrity checking and clean-up facilities should be sought.

l. Replication Triggers And Consistency

When replication is used (via DISP, etc.), mechanisms must be sought that control when an update takes effect in the target DSA. This is necessary to prevent loss of data integrity in a multi-processing environment caused by the data being “overwritten” while a Search operation is also in progress.

m. Performance Logs And Reports

DUAs and DSAs shall keep transaction logs that support performance management and system planning.

322. DUA Caching Guidelines

Employing DUA caching is a matter of national policy. When it is done, the guidelines in this paragraph may be followed.

a. Store cached information in nonvolatile memory.

b. Treat cached entries and cached certificates separately for the purpose of determining the useful life of the cached information. Extend the useful cache period for the certificate, since it is a relatively static entity with its own expiration time and revocation procedures.

c. Set the time-to-live for cached information according to the type of information stored in the cache (individual or organizational), the function of the command or persons operating the system, the maximum authorized message precedence, the security classification of the information and the DUA user, and the nature of the DUA.

d. Set the time-to-live for cached entries of individual users to expire within a 15 day time period. Set the time-to-live for cached entries of organizational users to have a maximum expiration period of four days.

e. Where an organizational user and individual user share the same DUA, the expiration for the limit on the time-to-live conforms to that for the organizational user. The local management center approves time-to-live values in excess of these recommendations.

f. Capture and record, with the cached entry, the date and time that the entry was last obtained in order to determine the expiration time of the entry.

g. Upon receipt of a CRL, all components containing cached certificates compare the cached certificates against the list of revoked certificates and purge those cached certificates matching the certificates listed in the CRL.

h. Cache expiration intervals are approved in advance by the local management center. This is to avoid saturation of the directory for inappropriate short intervals. The Local Center also requests that the cache maximum time limits be raised for conditions where the directory service is unable to provide adequate service.

i. Purge a cached certificate upon the expiration date contained within the certificate.

j. Cache knowledge information of DIB distribution in DSAs, unless it violates local security guidelines. This information may be used by DUAs to gain direct access to desired information.

SECTION VI

CHAINING

323. Chaining Policy

a. All Border DSAs and DSAs in combined task forces shall be capable of supporting both chaining and referrals.

b. Either chaining or referral may be used as long as performance and security requirements are met.

c. In the service controls, Prefer Chaining shall be the favored option. However, use of Chaining Prohibited is permitted.

CHAPTER 4

DIRECTORY SECURITY POLICES AND PROCEDURES

SECTION I

SECURITY

401. Security Services

a. The security services defined within this section have been developed as countermeasures against the perceived vulnerabilities of the X.500 model. This analysis was based on X.509, Annex B. The security services defined below are considered against the three general threats of unauthorized disclosure, modification, or unavailability of information contained in the directory. The information is vulnerable when held within a DSA or when transiting elements of the directory. The aggregation of the total information shared within the allied directory may raise the level of security risk, so although individual elements of information may be of low classification, the total system may have to be considered at higher classification.

b. Not all security services will be applied to the information within the directory. For example, confidentiality of information within the directory is only considered viable when a small amount of information is at a higher classification level than the rest of the directory and the information is to be shared amongst a small number of users.

c. Many applications and services will have requirements for security. Such requirements are derived from the need to protect the information from a range of potential threats. In order to protect against threats, security services shall be provided. These services are:

- Authentication
- Access Control
- Key Management
- Confidentiality
- Labeling
- Availability
- Integrity

402. Authentication

a. Peer entity authentication is performed between DUAs and DSAs and between DSAs to provide corroboration that a user or entity in a certain instance of communication is the one claimed. ACP 133 shall support mutual authentication through the use of strong authentication. Strong authentication relies on the use of asymmetric encryption. Asymmetric encryption uses the combination of a public component and a private component to sign digitally the credentials of the user or entity authenticating itself to the system. A digital signature guarantees both the origin and the integrity of the information that is digitally signed. This binding of the public key and its holder's identification information is conveyed through an X.509 certificate that is generated by a CA. Each individual nation shall implement its own CMI to include CAs in such a manner as to ensure the trusted path for certificate management. In the case of a CTF, authentication policies and procedures are under the control of the CTF commander.

b. The CMI is an integrated relationship of CAs and all the components necessary that operate under the authority of either a superior CA or, in conjunction with bilateral agreements, with other CAs.

c. The CMI includes the process for developing Certificate Policies. A Certificate Policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular Certificate Policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

d. Each CA shall have a statement of the practices, the CPS, which it employs in managing certificates.

e. Each nation's CPS shall identify the procedure used to create, maintain, and revoke credentials.

f. Two-way mutual peer-to-peer strong authentication shall be supported. Strong authentication shall be used in the Allied Directory System where warranted. ACP 133 shall support attributes for Version 3 X.509 certificates and Version 2 CRLs.

g. Assurance is incumbent on the availability of public keys in a way that guarantees that the public key really belongs to a particular identity. Validation of signatures is based on the assumption that the authenticating entity has the correct public key. The link between an identity and its public key shall be guaranteed. False identities and substituted keys are serious threats to these mechanisms. Each CMI's CPS shall ensure that actions are taken to mitigate these threats.

h. Within the ACP 133 Directory system, all DSAs shall be able to process bind requests that are simply authenticated and those that are strongly authenticated, utilizing an agreed upon digital signature algorithm. DSAs shall support access control policy that prevents unauthorized disclosure or modification of information based on the level of authentication used. The DSA shall strongly authenticate itself to its communication peer (i.e., DSAs, DUAs, and management

entities) as required. The success or failure of the steps in the authentication process shall be audited and stored in the DSA audit database to facilitate compromise recovery and to enhance security of the Directory.

i. In the Allied Directory, the following additional security constraints shall be met.

(1) Prior to exchanging any information, any pair of DSAs shall strongly authenticate themselves to each other if required by security policy between the two DSAs. Additionally, the DSAs shall not permit access to any information until all access control checks have been performed and granted.

(2) Only approved cryptographic mechanisms for the DSA application and the associated processes shall be used.

(3) The DSA shall support a CMI-defined signature validation process. This process shall include validating the CA which produced the certificate used to sign the identification and authentication information (i.e., validate the certification path).

(4) If the claimed identity is not validated, the request shall be rejected and the failure audited. Additional security actions may also be initiated; for example, the DSA may lock out the user.

(5) In those environments where Rule-based Access Control (RBAC) is imposed, each entity shall exchange privilege/authorization information required for the access control decision function, when performing the strong authentication Bind operation.

(6) Once the communications partners have successfully authenticated themselves to each other, the DSA shall limit access to information stored within its DSA according to the parent (host) system security policy.

(7) The DSA shall allow access and privileges to be set only by an authorized management entity.

403. Access Control - General

a. The X.500 Directory standard defines three access control schemes: Simplified Access Control, Basic Access Control (BAC), and RBAC. However, how that information is stored within a country's directory is a national issue. The ACP 133 shall mandate that directory systems ensure that the agreed-upon access controls are maintained.

b. The access control mechanisms shall include both RBAC as well as BAC. RBAC restricts access to objects within the directory by use of predefined labels to enforce access rights to information stored within the Directory. User or end-entity authorization information may be exchanged through extensions to the Version 3 X.509 certificates. ACI about the target (data within the DIB) shall be conveyed through the use of sensitivity labels. The format and processes associated with the privilege/authorization information are defined within each CMI's

CPS. The format and processes associated with security labels are defined in an Annex of ACP 120.

c. Within the Allied Directory Service there is a requirement to hold information at different levels of protective marking, and therefore, it is necessary to have a method by which the confidentiality of the information can be maintained without disclosure to unauthorized access. In addition, there may be occasions where information will be stored in a Directory that is of a higher classification than that which the DSA normally supports, or is of a sensitive nature and requires separation from disclosure to system administrators and other authorized users. This requirement shall be supported by one of the following mechanisms, in accordance with security policy:

- encryption of the stored information to protect its content from unauthorized disclosure
- access control mechanisms to protect the stored information from unauthorized access
- the use of both services

404. Basic Access Control

a. BAC is based on a relatively simple concept: either a list of users and the permissions to which they are entitled, or a list of protected items and the permissions necessary to access them, is held within the directory. This information is contained within ACI items. ACI items can be held within a number of parts of the directory depending on their intended usage and sphere of influence.

b. Each ACI item consists of four parts.

(1) Identification tag is used to name a particular ACI item.

(2) Precedence level is a number which determines the order in which ACI items should be considered. An item with a higher precedence will overrule an item with a lower precedence.

(3) Authentication level is the level to which the user must be authenticated. This can be no authentication, simple authentication, strong authentication, or by some external method.

(4) Either Item first permissions, which lists a set of protected items, and the set of users, all potentially with varying permissions, or User first permissions which lists a set of users and the protected items, all potentially with varying permissions that the users may or may not access is the fourth part.

405. Rule-based Access Control

a. Within ACP 133 and the civil standards arena, a requirement for additional information to be included in determining whether access can be granted or denied to an object has been identified. This is defined as RBAC, and requires administratively imposed access control policies to be applied to the contents of the directory.

b. RBAC uses security labels that can be attached (by securely binding the label to the information using a digital signature) to attribute values stored within the directory. The security label of an attribute shall be bound to the attribute value using a digital signature. This label can then be used to determine whether a user may access protected information. RBAC can be used alone, or in conjunction with BAC. Refer to clause 17.4.3 in ITU-T Rec. X.501 (1997) | ISO/IEC 9594-2: 1997.

c. RBAC adds the following constraints on the access control decision.

(1) DiscloseOnError is not supported under RBAC, and hence if Read access is denied, then the operation acts as if the entry does not exist.

(2) RBAC affects operations on reading attribute values (e.g., Read and Search) in that the attribute value is not visible if access is not authorized (operation is carried out as though the attribute value is not present). It does not currently affect operations on entries as a whole which do not impact on existing attribute values (e.g., Add Entry).

(3) RBAC operations which involve removing an attribute value (e.g., Remove Entry, Modify Entry, and Remove Attribute) fail if the access is not authorized.

(4) If access to all attributes of an entry is denied under RBAC, access is denied to that entry for all operations.

d. An error code is returned from an operation or the attribute value, attribute type, or entry is omitted from the operation result if:

- the label for the attribute value denies access, then the attribute value is hidden
- the labels for attribute values of a given type deny access, the existence of the attribute is hidden (If access is denied to all attribute values of a type, then access is denied to that type.)
- the labels for attribute values of a given entry deny access, the existence of the entry is hidden (If access is denied to all attribute values of an entry, then access is denied to that entry.)

e. To enforce RBAC, initiator-bound access control information (clearance information) needs to be provided to enable a comparison to be made with the target's security label. Clause 17.5 of ITU-T Rec. X.501(1997) | ISO/IEC 9594-2: 1997 identifies the syntactic representation

for the clearance attribute. There are at least two methods to convey this information with integrity.

(1) The user's clearance can be bound to the user's DN and the public key used to authenticate that DN with a public key certificate extension.

(2) The user's clearance can be bound to the user's DN and to the user's X.509 certificate using an attribute certificate.

f. If the first method is chosen, and the authority verifying the public key information of a user may or may not be the same authority that is responsible for issuing and verifying a user's clearance, the clearance must be supplied to the CA in a trusted manner.

g. Each CMI's CPS shall include the procedures required to validate each end-entity's identity and privilege/authorizations.

h. The security labels will be based on a hierarchical set: UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET, that can be compared to the clearance of the requester based on a corresponding set of hierarchical class values. These hierarchical classifications form the "base set" for the RBAC scheme and will be extended to address privilege information conveyed in a security category and/or privilege marking.

i. In resolving permissions, the DSA shall first obtain the clearance of the user from a trusted source. This information shall be conveyed during the authentication process. When obtained, the contents of the security label is checked against the user's clearance. RBAC does not define what type of subsequent operations may be performed, e.g., modify, remove etc.

406. Access Control Decision Function

a. In the event that RBAC has been implemented, additional steps in the access control transforms must occur. First, the hierarchical clearance of the user must dominate the hierarchical classification of the label. Second, if additional categories have been applied to the security label, there must be a comparison function between the security categories component of both the data label and the user clearances. If RBAC succeeds and there are no additional RBAC restrictions imposed, the user is granted access. The security policy rules defining the relationship between the end-entity's privilege/authorization set and the security label shall be provided by each nation's appropriate authority.

b. The Access Control Decision Function (ACDF) specifies how ACI items shall be processed in order to determine whether access should be granted for a particular operation.

c. Figure 4-1 and Figure 4-2 are based on the ISO/IEC 10181-3 Security Framework in Open Systems standard (Part 3 - access controls), but have been adapted to fit the BAC model described in the X.500 standard. The ACDF makes the decision as to whether to grant or deny access to the requested object(s) by applying pre-defined access control policy rules to an access request.

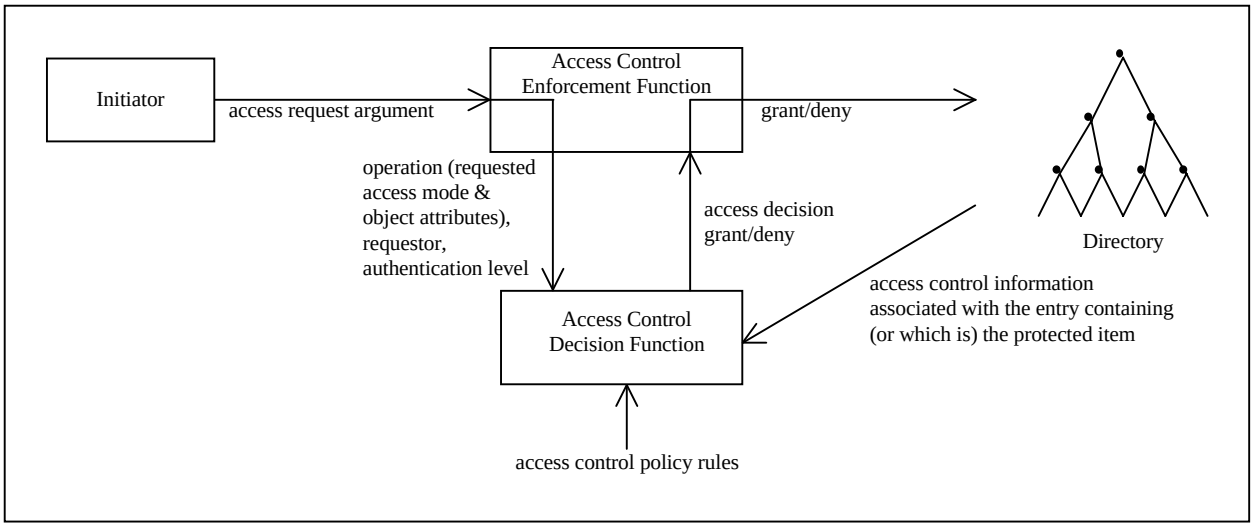

Figure 4-1
Diagram of ACDF Required for Basic Access Control

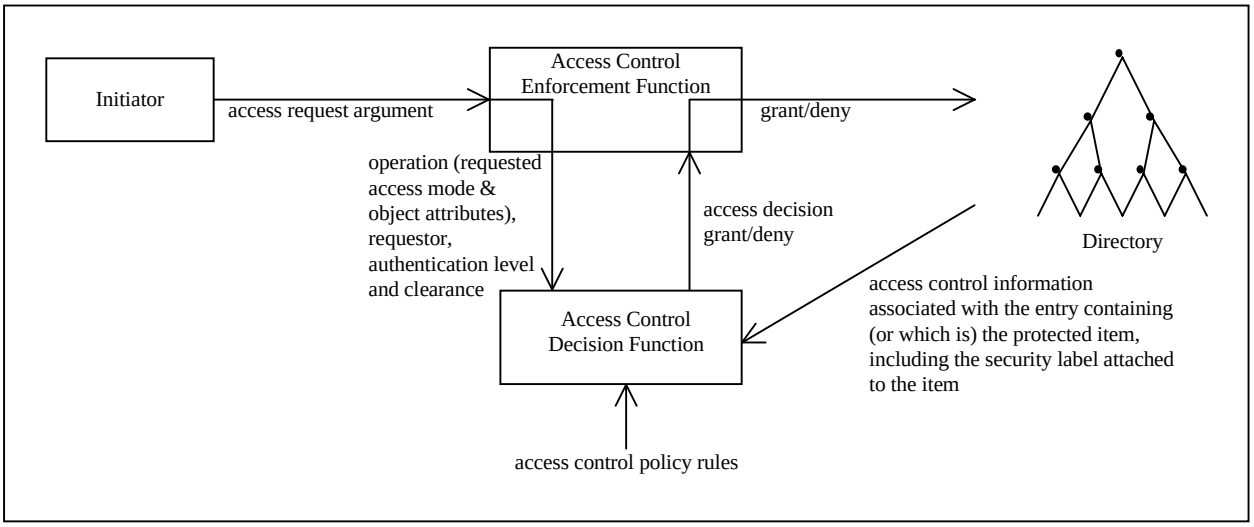

Figure 4-2
Diagram of ACDF Required for Rule-based and Basic Access Control

d. If RBAC is being used in conjunction with BAC, then RBAC should always take precedence over the BAC. Therefore, if RBAC scheme rules do not allow access to a requested operation, then the operation will be denied independently of whether access would have been granted under the BAC scheme. Only if the RBAC scheme rules allow access to a requested operation will the ACDF for BAC be executed to determine if access should be granted.

e. A policy identifier shall be used to identify under which security policy the clearance and security labeling are being enforced.

f. The security policy is represented by an object identifier that indicates the security policy the subject supports. Each security policy registered shall have documentation that indicates the values of classifications and privilege/authorization sets valid within the context of that security policy.

407. Key Management

a. Common cryptographic algorithms and their intended usage need to be supported. National CPS will define acceptable cryptographic algorithms and required usages.

b. In the event that a DSA's signature or confidentiality keys are compromised, immediate notification to the Security Authority shall occur.

408. Confidentiality

a. In some situations, the Allied Directory may not give sufficient assurance that data is kept confidential in storage, regardless of access controls. Confidentiality of attributes in storage is provided through use of:

- a template for the definition of attributes which are protected by a security transformation which provides confidentiality (Refer to Clause 18.2.2 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.)

- an attribute for distributing keys to those who need to decrypt attributes using the identified key. The key being distributed is protected by encrypting the key value with the public key of each authorized reader of the attribute. (Refer to Clause 18.2.3 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.)

b. Note: Other mechanisms can be used to distribute the keys required to protect attributes defined using the Encrypted Attribute Value template.

409. Labeling

a. General

A common policy on labeling and clearance is the basis for labeling in the Allied Directory. The format and processes associated with security labels are defined in an Annex of ACP 120. Labeling and clearance information implemented in the Allied Directory Services shall support access control in the shared information environments.

b. Security Classification

(1) The following security classifications are valid:

- UNCLASSIFIED
- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

(2) These classifications are hierarchical and are listed in ascending order, that is, Restricted is a higher classification than UNCLASSIFIED.

(3) Within subject Clearances issued to end-entities, the following classifications are valid:

- UNCLASSIFIED
- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

(4) These clearances are listed in hierarchical order with Top Secret dominating Secret and so on. A Top Secret clearance allows access to all other information unless other restrictions apply. The rules governing the population of the clearance attribute are defined in each CMI's certificate policy.

c. Categories

(1) Categories may be divided into multiple groups. At a minimum, the following types shall be supported: Restrictive, Permissive, and User-Defined.

(2) A Restrictive Category requires that all values present in the security label shall be present in the authorizations conveyed in the clearance.

(3) Permissive Categories require that at least one value present in the security label shall be present in the authorizations conveyed in the clearance. This is applicable when indicating the capability to constrain access by nationality, for example, Release To or Eyes Only.

(4) User-Defined Categories shall be identified when implemented across international boundaries.

(5) An ACDF matches the user or end-entity's clearances and the attribute security label to determine if the user or end-entity is allowed to access the attribute value. The permissive categories are checked by access control functions to ensure that if any one of the bits in the extension match the bits in the security label, the attribute can be accessed. The restrictive categories are used by access control functions to ensure that all bits in the certificate extension match all the bits in the label prior to granting access. The user-defined categories shall process in accordance with the registered procedures.

d. Privacy Markings

Privacy markings are text handling instructions and warnings. They provide no support for access control decisions.

e. Policy Identifiers

(1) The set of the categories and classifications and their semantic interpretation is defined in context of the policy identifier.

(2) Multiple security policies will exist and need to be supported. Equivalency mapping will be identified through the cross certification processes.

410. Availability

Availability of the data in the Allied Directory System shall be ensured through robust replication and disaster recovery practices.

411. Integrity

a. Data integrity provides proof of the integrity of the information, either in storage or while in communications channels. The mechanism involves encipherment of a compressed string of the relevant data to be stored or transferred. This will be a function of the digital signature mechanisms using an asymmetric scheme.

b. In the event integrity is required on information stored in the directory, the information shall be signed. The user who requires validation of the integrity of that information shall validate the signature to ensure no unauthorized modifications have occurred. The definition of an attribute type to hold a digital signature, along with associated control information, which provides integrity of a whole entry or all values of selected attribute types is found in clause 18.1.2 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.

c. The Allied Directory shall support integrity on a single attribute value. The definition of the Attribute Value Integrity Information Context is found in Clause 18.1.3 of ITU-T X.501 (1997) | ISO/IEC 9594-2: 1997.

d. The Allied Directory shall be capable of supporting signed operations on all operation requests received, as well as generate signed responses to those arguments. This shall include error responses. The integrity protection required shall be negotiated and agreed-upon when establishing connectivity. For those combined task force environments that cannot support the required protection, then the information may be returned unprotected. The decision to utilize the information is up to the policies of the task force commander.

SECTION II

ACCOUNTABILITY/AUDITING

412. Data Protection

Any of the information that is stored within a Security Management Information Base (SMIB) shall be protected against manipulation or destruction by unauthorized users or end entities. Changing any of the thresholds associated with collection of audit information shall be made available only to those authorized audit management entities. When information from one domain is replicated into another domain, the agreement to shadow shall contain details on how archive of and access to audit data will be supported.

CHAPTER 5

DIRECTORY MANAGEMENT POLICIES AND PROCEDURES

501. Scope

a. The policies defined in this document for management are applicable to the directory system component level of the Allied Directory System. Additional requirements such as help desks and operations relating to the higher level system issues of the Allied Directory System will be covered in related documents.

b. There are three operational areas of management to consider.

(1) Management of each nation's domain shall be done at the national level and is out of the scope of this document.

(2) Management of a combined domain shall be done in accordance with this ACP and under the control of the commander of the CTF.

(3) Management of the international domain, such as the management of Border DSAs shall be performed as defined in this ACP and other Allied documents.

502. Mandated Functionality

For the purposes of insuring a base level of management functionality within the Allied Directory System components, the following features and functions are mandated.

a. All DSAs and DUAs shall be capable of extending the schema to include new object classes and attributes and, optionally, new syntaxes without recourse to software rework.

b. All DSAs shall be able to have ACI and other subentry information configurable.

c. All DSAs shall be able to have their replication agreements configurable.

d. All DSAs shall support logging facilities as defined in paragraph 504.

e. All DSAs shall support, as a minimum, the X.500 Directory Monitoring Management Information Base (MIB) defined in RFC 1567, or equivalent.

f. All DSAs shall support the generation of events or alarms and log entries that reflect error conditions such as resource problems, protocol failures, or system security violations. Sample alarms include:

- security violations (unable to authenticate DUA-DSA or DSA-DSA)
- connection failure

- resource limits encountered
- process error

g. All DSAs shall provide a management console interface that will permit local and remote management. Remote management facilities shall be applied with some authorization and protection mechanism.

503. Desirable Additional Functionality

The following additional features and functions are desirable.

a. DUAs should be configurable by a system administrator to control the services that are permitted to the DUA user. Note that the Allies intend to control the extent of DAP operations by DUAs by configuring the DUA and by access control information in the DSA.

b. Management interfaces of Directory components should apply standard protocols such as DAP, CMIP and/or SNMP.

c. Management logs and log controls should reflect the functionality defined in ITU-T Rec. X.735 | ISO/IEC 10164-6.

d. Management facilities provided with directory components should relate to directory domains, i.e., multi-DSA systems.

504. Event Logs

a. DSAs shall provide for the logging of all operations with various levels of detail. Log control mechanisms shall provide configuration or functions for:

- controlling the size of log
- action taken when a file is full, e.g., overwrite the log or create a new file
- deleting or archiving the log
- controlling logging levels
- starting and stopping logging

b. Log entries shall provide:

- event time
- event type
- operation type (e.g., List, Modify, Modify DN)

- originator's DN
- target object
- outcome of request or response, i.e., success, failure, error, etc.
- major parameters:
  - service controls
  - filter used
  - security parameters
  - entryInformationSelection

c. DSAs shall support recording the following errors:

- errors defined in clause 12 of X.511, such as, nameError, updateError, attributeError, securityError, abandoned, abandonFailed
- errors defined in clause 12 of X.525, such as, shadowError. Sample problems are unsupportedStrategy and inactiveAgreement.
- errors defined in clause 24 of X.501, such as, operationalBindingError. Sample problems are invalidAgreement and notAllowedForRole.
- errors defined in clauses 11 - 13 of X.518, such as, dsaReferral

505. Service Level Agreements

A SLA is the formal agreement to be used between Allies for the operation of an ACP 133-compliant directory. Such agreements shall be established on a bilateral basis between Allies and shall address the quality, quantity, and, where appropriate, the cost of the directory service to be established. An SLA shall include sufficient definitions and measures of performance to cover the type of service, the quantity and quality of the service required, and any time-scale targets. In principle, SLAs should be written to a common format and, to this end, a suggested outline is given in Annex F.